Thema: Risikomanagement in kleinen und mittleren Unternehmen - was ist sinnvoll?

13. April 2018

Inhaltsverzeichnis

Inhaltsverzeichnis **2**

Abbildungsverzeichnis **3**

1 Einleitung **4**
1.1 Grundlagen 5

2 Anforderungen aus Gesetzen, Normen und Verordnungen **6**
2.1 GmbH-Gesetz 6
2.2 Bürgerliche Gesetzbuch 7
2.3 Produkthaftungsgesetz 7
2.4 Handelsgesetzbuch 7
2.5 IT-Sicherheit 8
2.6 Personenbezogene Daten 9
2.7 Gleichbehandlung 9
2.8 Arbeitsschutz 9
2.9 Urheberrecht 9
2.10 Anforderungen aus Normen 9

3 Unternehmensrisikomanagement **11**
3.1 Risikopolitik 11
3.2 Bedarfsanalyse 13
3.2.1 Mittlere Unternehmen 13
3.2.2 Kleine Unternehmen 14
3.3 Analyse der Sicherheitsanforderung 15
3.4 Implementierung 15
3.5 Überprüfung 19

4 Zusammenfassung der Ergebnisse **20**

Literaturverzeichnis **22**

Abbildungsverzeichnis

3.1 Strategien für das Supply-Chain-Risikomanagement in deutschen Unternehmen, Eigene Darstellung 12
3.2 Risikomanagement im Einkauf der Möbelindustrie, Eigene Darstellung 12
3.3 Detaillierungsgrad des Risikomanagement bei KMU 14
3.4 Produkt/Dienstleistung in Beziehung der Umwelt 15
3.5 Risikoidentifizierung 16
3.6 Risikofaktoren 17
3.7 Risikoprioritäten KMU 19

Kapitel 1

Einleitung

Ein funktionierendes Risikomanagement wird in Unternehmen zunehmend bedeutsam und wird somit für Management-Ebenen immer wichtiger. Auf Grund zunehmender gesetzlicher Vorgaben und branchenspezifischen Regularien ist ein wirtschaftliches und durchgängiges Risikomanagement in jedem Unternehmen erforderlich. So sind Produktions und Fertigungsprozesse ohne IT kaum mehr denkbar um wettbewerbsfähig zu bleiben. Was im Gegenzug ein Unternehmen verwundbar und angreifbar macht und hohe Schäden verursachen kann. Bedrohungen für Unternehmen sind weitreichend und können von Stromausfällen, IT-Ausfällen, Computerkriminalität, Einbruch, Personalmangel oder Lieferantenausfälle bis hin zu kompletten Produktionsausfällen reichen. Die Ausfallkosten können hierbei leicht die Millionenhöhe überschreiten, wenn interne und externe Folgekosten berücksichtigt werden. Das bedeutet, Unternehmen müssen sich vor Ausfällen jeglicher Art schützen, um so gesamtunternehmerische Risiken auszuschließen. Ein funktionierendes Risikomanagement stellt daher ein zentralen Erfolgs- und Überlebensfaktor für Unternehmen dar.

Jedoch stellt sich die Frage: Inwieweit kleine und mittlere Unternehmen (KMU), angesichts der zur Verfügung stehenden Ressourcen ein eigenes Risikomanagement umsetzen können? Die Risikotragfähigkeit[1] ist bei kleinen Unternehmen wesentlich kleiner als bei mittleren Unternehmen, da Ausfallkosten oder Schadenskosten schneller zur Insolvenz führen können.

Ziel dieser Arbeit soll sein, die Wege zum Unternehmensrisikomanagement aufzuzeigen und dabei speziell ein für KMU umsetzbares Risikomanagement zu erarbeiten. Dabei werden die gesetzlichen Anforderungen verschiedener Branchen betrachtet und geprüft ob es ausreichend ist, sich auf gesetzliche Vorgaben allein zu verlassen und inwieweit ein Risikomanagement vorzusehen ist. Es soll aufgezeigt werden, wie unternehmerische Prozesse anhand der jeweiligen Risikopolitik zu untersuchen sind und mit einer geeigneten Strategie im Unternehmen zu implementieren sind.

[1] Risikodeckung besteht aus dem Kapital, den die Gesellschafter bereit sind im Krisenfall „zu opfern"

1.1 Grundlagen

Das Risikomanagement definiert und beschreibt, wie unternehmerische Gefahren und Chancen gemanagt werden. Untersucht systematisch Prozesse, identifiziert potentielle Unternehmensrisiken und schafft Lösungen um diese zu minimieren oder sogar komplett zu beseitigen. Risikomanagement ist demnach eine notwendige Strategie zur operativen Tätigkeit von Unternehmen. Denn um so später ein Risiko erkannt wird, um so kostenintensiver fallen korrektive Maßnahmen aus [Mul13]. Ein funktionierendes aufgebautes Risikomanagement ist demnach ein ideales Werkzeug um frühzeitig Kostenrisiken zu identifizieren. Bei frühzeitig erkannten Risiken können entsprechende kostengünstigere Gegenmaßnahmen implementiert werden, welche dann entsprechende Wirkung während der Geschäftstätigkeit entfalten [Bra15].

Das Risikomanagement muss auf den Unternehmenszweck, der mittel- und langfristigen Ausrichtung, vom Umfeld und von der strategischen Positionierung des Unternehmens abgestimmt werden. Insbesondere in internationalen Unternehmen ist die Gestaltung einer gleichen Risikokultur von Bedeutung, da je nach Kultur die Risikowahrnehmung unterschiedlich ausgeprägt sein kann und somit eine geringe oder hohe Risikobereitschaft besteht [Bra15].

Die Geschäftsleitung muss unter Berücksichtigung der Risikobereitschaft die Risikopolitik des Unternehmen in entsprechenden Regeln oder Leitlinien festlegen. Durch den aktuell sich stetig verändernden technologischen Fortschritt und der zunehmenden Vernetzung und Globalisierung muss die Risikopolitik des Unternehmens stetig neu bewertet und entsprechend angepasst werden. Technologische Entwicklungen wie Produkte zur Industrie 4.0[2], wie auch andere neue Entwicklungen, erzeugen neue der Herausforderung der Informationstechnik (IT) Durchdringung. Daraus ergeben sich neue, zu bewältigende Herausforderungen, besonders in der IT-Sicherheit [Mül15].

[2]Beschreibt den vierten Evolutionsschritt der Industrie mit der datentechnische Vernetzung von Sensoren, Maschinen und Produktionsbetrieben

Kapitel 2

Anforderungen aus Gesetzen, Normen und Verordnungen

Ob Klein oder Groß - Gesetze, Verordnungen und Normen gelten für alle Unternehmensgrößen. Der Unterschied zwischen großen und kleinen Unternehmen besteht im wesentlichen darin, dass sich Umfang sowie der Detaillierungsgrad unterscheidet. Bei größeren Unternehmen kommt hinzu, dass diese teilweise unterschiedliche Standorte, mehrere Verwaltungen oder verschiedenartige Produktionsanlagen oder komplexe IT-Infrastruktur besitzen, wohingegen bei kleinen Unternehmen die Sicherheitsanforderungen wesentlich abnehmen aber dennoch vorhanden sind [Mül15]. Als KMU werden Unternehmen definiert, in denen weniger als 250 Angestellte tätig sind und deren Jahresumsatz von 50 Mill. Euro nicht überschreitet. Die Arbeit soll sich auf Verarbeitendes Gewerbe und Handel sowie Dienstleistungen beschränken, da diese den größten Anteil der KMU bilden [Sta16].

Die externen Anforderungen an das Risikomanagement sind umfangreich und vielfältig und ergeben sich beispielsweise aus den Bereichen Arbeitssicherheit, Datenschutz, Buchführung, Bilanzierung, Urheberrecht sowie branchenspezifischen Anforderungen. Diese entstanden aus unterschiedlichen Branchen und sind teilweise in den einzelnen Ländern überlappend, was bei Risikopolitik der Unternehmen entsprechend berücksichtigt werden muss [Mül15].

Um die Arbeit überschaubar zu halten, wird nur auf nachfolgende externe Anforderungen, welche die Geschäftstätigkeit im Deutschen Raum betreffen eingegangen [Bun]. Bei International agierenden Unternehmen müssen weitere landesspezifische Gesetze, Verordnungen und Normen berücksichtigt werden.

2.1 GmbH-Gesetz

Im GmbH-Gesetz wird in § 43 die „Haftung der Geschäftsführer“ geregelt. Das bedeutet, dass der ordentliche Geschäftsmann eine Sorgfaltpflicht zu erbringen hat. Bei Verletzung haften die Gesellschafter (Abs. 2). In § 41 wird die Buchführungspflicht der Geschäftsführer geregelt.

In der Abschlussprüfungs-Richtlinie „EuroSOX“ 2006/43/EG „Abschlussprüfungen von Jahresabschlüssen und konsolidierten Abschlüssen“, Abs. 24 regelt „Prüfungsausschüsse und ein wirksames internes Kontrollsystem tragen dazu bei, finanzielle und betriebliche Risiken sowie das Risiko von Vorschriftenverstößen auf ein Mindestmaß zu begrenzen und die Qualität der Rechnungslegung zu verbessern“ [Mül15].

2.2 Bürgerliche Gesetzbuch

Das Bürgerliche Gesetzbuch (BGB) regelt in § 280 den „Schadensersatz wegen Pflichtverletzung“ [Mül15]. Hieraus ergibt sich für die Geschäftsleitung, dass Vorkehrungen zu treffen sind, damit es zu keiner Pflichtverletzung kommt.

§ 433 regelt die „Vertragstypische Pflichten beim Kaufvertrag“. Abs (1) „Durch den Kaufvertrag wird der Verkäufer einer Sache verpflichtet“

Wenn Unternehmen für Ihre Kunden Leistungen verkaufen, können sicherheitsrelevante Anforderungen in Dienstverträgen (vgl. BGB § 611) oder in Werksverträgen (vgl. BGB § 631) geregelt werden.

2.3 Produkthaftungsgesetz

Im Produkthaftungsgesetz (ProdHaftG) heißt es in § 1 Abs. 1 „Wird durch den Fehler eines Produkts jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Hersteller des Produkts verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen.“ sowie im Umwelthaftungsgesetz (UmweltHG) § 1 Abs. 1 „Wird durch eine Umwelteinwirkung, die von einer im Anhang 1 genannten Anlage ausgeht, jemand getötet, sein Körper oder seine Gesundheit verletzt oder eine Sache beschädigt, so ist der Inhaber der Anlage verpflichtet, dem Geschädigten den daraus entstehenden Schaden zu ersetzen.“. Es haftet in diesem Fall das Unternehmen, sollte dieses nicht entsprechend Maßnahmen ergriffen haben um diese Risiken auszuschließen. Für die Herstellung für Maschinen gilt unter anderem im Produkthaftungsgesetz die Maschinenrichtlinie 2006/42/EG, welche in Verbindung mit Normen (Kapitel 2.10 auf Seite 9) die Anforderungen verfeinert [Mül15].

2.4 Handelsgesetzbuch

Gemäß Handelsgesetzbuch (HGB) § 238 gilt die „Buchführungspflicht“ worin „jeder Kaufmann verpflichtet ist, Bücher zu führen und in diesen seine Handelsgeschäfte und die Lage seines Vermögens nach den Grundsätzen ordnungsmäßiger Buchführung ersichtlich zu machen“. In HGB § 238 Abs. 2 heißt es weiter „Die Eintragungen in Büchern und die sonst erforderlichen Aufzeichnungen müssen vollständig, richtig, zeitgerecht und geordnet vorgenommen werden.“

Im Handelsgesetzbuch in § 289 wird der „Inhalt des Lageberichts“ den jede Kapitalgesellschaft zu erbringen hat spezifiziert. Abs 1„a.) die Risikomanagementziele und -methoden der Gesellschaft einschließlich ihrer Methoden zur Absicherung aller wichtigen Arten von Transaktionen, die im Rahmen der Bilanzierung von Sicherungsgeschäften erfasst werden, b) die Preisänderungs-, Ausfall- und Liquiditätsrisiken sowie die Risiken aus Zahlungsstromschwankungen, denen die Gesellschaft ausgesetzt ist.“

Weiterhin regelt das HGB in § 257 „Aufbewahrung von Unterlagen, Aufbewahrungsfristen“, „Demzufolge sind z. B. Handelsbücher, Inventare, Jahresabschlüsse, Lageberichte, Konzernabschlüsse, Konzernlageberichte sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen sowie Buchungsbelege zehn Jahre lang aufzubewahren “[Mül15].

2.5 IT-Sicherheit

Der Gesetzesentwurf zur IT-Sicherheit aus dem Jahr 2014 definiert für kritische Infrastrukturen Sicherheitsbestimmungen wie „Einrichtungen, Anlagen oder Teile davon“ die „den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz-und Versicherungswesen angehören und“ ... „von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden“. Weiter heißt es in § 8a „Betreiber Kritischer Infrastrukturen sind verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Absatz 1 angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. Dabei ist der Stand der Technik zu berücksichtigen. Organisatorische und technische Vorkehrungen sind angemessen, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen Kritischen Infrastrukturen steht“.

Weiterhin beschreibt das Institut der Wirtschaftsprüfer (IDW) im IDW-RS-FAIT-1 „Grundsätze ordnungsmäßiger Buchführung bei Einsatz von Informationstechnologie“, dass (88) „Ein Ausfall wesentlicher IT-Anwendungen ohne kurzfristige Ausweichmöglichkeit kann materielle und immaterielle Vermögensschäden nach sich ziehen und stellt einen wesentlichen Mangel der Buchführung dar“. Weiterhin heißt es in IDW-RS-FAIT-3 „Grundsätze ordnungsmäßiger Buchführung beim Einsatz elektronischer Archivierungsverfahren“, beschreibt in Kapitel 6.3 „Sicherheitsanforderungen“ erforderliche IT Maßnahmen wie Zugriffskontrollen, Schutz vor Manipulation, Verfügbarkeit oder Autorisierung.

2.6 Personenbezogene Daten

Im Bundesdatenschutzgesetz (BDSG, Federal Data Protection Act) sind die Anforderungen an den Schutz personenbezogener Daten festgelegt. § 4b verbietet dabei die Übermittlung personenbezogener Daten wenn ein „angemessenes Datenschutzniveau nicht gewährleistet“ ist.

EU-Datenschutzrichtlinie 95/46/EG Artikel 1 ist der Schutz festgelegt: „Schutz der Grundrechte und Grundfreiheiten und insbesondere den Schutz der Privatsphäre natürlicher Personen“.

2.7 Gleichbehandlung

Im allgemeinen Gleichbehandlungsgesetz (AGG) regelt § 1 „Ziel des Gesetzes ist, Benachteiligungen aus Gründen der Rasse oder wegen der ethnischen Herkunft, des Geschlechts, der Religion oder Weltanschauung, einer Behinderung, des Alters oder der sexuellen Identität zu verhindern oder zu beseitigen“ [Mül15].

2.8 Arbeitsschutz

Das Sozialgesetzbuch VII (SGB VII), das Arbeitsschutzgesetz (ArbSchG), das Arbeitssicherheitsgesetz (ASiG), die Arbeitsstättenverordnung (ArbStättV), die Betriebssicherheitsverordnung (BetrSichV), die Bildschirmarbeitsverordnung (BildscharbV), sowie die Vorschriften Deutsche Gesetzliche Unfallversicherung (DGUV) stellen in Deutschland die Anforderungen an Arbeitsschutz und -sicherheit [Mül15]

2.9 Urheberrecht

Das Urheberrechtsgesetz (UrhG), das Markengesetz (MarkenG) und das Patentgesetz (PatG) schützt „Die Urheber von Werken der Literatur, Wissenschaft und Kunst genießen für ihre Werke Schutz nach Maßgabe dieses Gesetzes ... Zu den geschützten Werken der Literatur, Wissenschaft und Kunst gehören insbesondere: Sprachwerke, wie Schriftwerke, Reden und Computerprogramme, ... Darstellungen wissenschaftlicher oder technischer Art, wie Zeichnungen, Pläne, Karten, Skizzen, Tabellen und plastische Darstellungen“

2.10 Anforderungen aus Normen

Über gesetzliche Anforderungen hinaus stellen Normen, welche als anerkannte Regeln der Technik gelten, weitere Anforderungen in den jeweiligen Branchen. Europäische Normen müssen von allen Mitgliedsstaaten in das nationale Normenwerk übernommen werden. Das Deutsche Institut für Normung (DIN) ist die

zuständige Institution der Bundesrepublik Deutschland. Wichtige Normen, im Bezug auf die heutige IT-Durchdringung in Unternehmen, sind die Normen ISO/IEC-27000 Standards der IT-Sicherheit, BSI[1]-Standard 100-3 Risikoanalyse auf der Basis von IT-Grundschutz, ISO 28000 Sicherheitsmanagementsysteme für die Lieferketten und weitere.

Speziell das Risikomanagement für Unternehmen wird in der Norm ISO/IEC-31000-Reihe beschrieben. Die ISO 31000 beschreibt im wesentlichen den Plan-Do-Check-Act-Zyklus[2] um ein Risikomanagementprozess anzuwenden. Risikoidentifikation, Risikoanalyse, Risikobewertung sowie Risikosteuerung und Überwachung sind die wesentlichen Schritt der ISO 31000 Norm [Mül15].

[1] Bundesamt für Sicherheit in der Informationstechnik

[2] PDCA-Zyklus beschreibt einen iterativen vierphasigen Problemlösungsprozess

Kapitel 3

Unternehmensrisikomanagement

3.1 Risikopolitik

Im Kapitel 2 wurde festgestellt, dass Anforderungen aus Gesetzen und Normen individuell zur jeweiligen Branche anzuwenden sind. Ein verpflichtendes Risikomanagement für KMU wird nicht vorschrieben, sich auf gesetzliche Vorgaben allein zu verlassen ist daher nicht ratsam. Dieser Aufgabe, zur Bildung der Risikostrategie obliegt der Unternehmensleitung, welche Ziele und Verantwortlichkeiten anhand einer Risikoanalyse (Plan) die eigene Risikopolitik (Do) definiert. Ein Risiko-Controlling sowie -reporting (Check), integriert in Entscheidungsprozessen, rundet den PDCA-Zyklus ab (siehe Kapitel 2.10) [Bra15]. In kleinen Unternehmen ist Risikomanagement in der Regel Chefsache.

Es gibt sich jedoch die Frage: Inwieweit kleine und mittlere Unternehmen (KMU), angesichts der zur Verfügung stehenden Ressourcen ein eigenes Risikomanagement umsetzen können? Inwieweit erfolgt die Risikoanalyse in KMU? Welche Risikopolitik wird verfolgt?

Die nachfolgende Studie[Sta16] in Abbildung 3.1 zu Strategien für das Supply-Chain-Risikomanagement von 189 befragten deutschen Unternehmen aus den Jahr 2012 gibt Aufschluss, dass Unternehmen dahingehend bestrebt sind ihre Wertschöpfungskette[1] der Kerngeschäftsprozesse aufrecht zu erhalten. Es ist davon auszugehen, dass dies durch existierende Lieferverträge herrührt (Siehe Kapitel 2.2), dass Unternehmen bestrebt diese zu erfüllen da es im Falle eines Lieferausfall zur Forderungskosten seitens Kunde kommen kann.

Eine weitere Studie aus dem Jahr 2010 ergab, dass im Einkauf der Möbelindustrie nur 43 % der befragten 104 Unternehmen Maßnahmen zur Risikominimierung durchführen. Das lässt sich dadurch erklären, dass die Möbelindustrie eher durch Zeit unkritische Supply-Chains geprägt ist und daher weniger Maßnahmen zur Risikovermeidung im Supply-Chain benötigt. Abbildung 3.2 zeigt die Ergebnisse der Umfrage.

[1] Die Wertschöpfungskette (Value Chain) nach Michael E. Porter stellt die Stufen der Produktion als eine geordnete Reihung von Tätigkeiten dar.

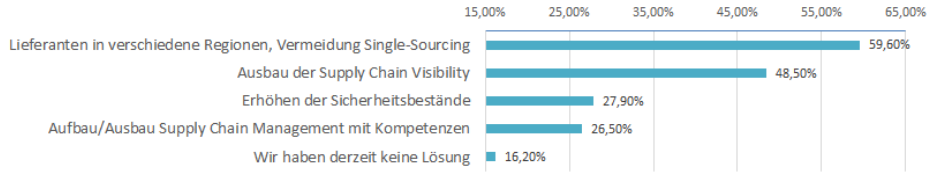

Abbildung 3.1: Strategien für das Supply-Chain-Risikomanagement in deutschen Unternehmen, Eigene Darstellung

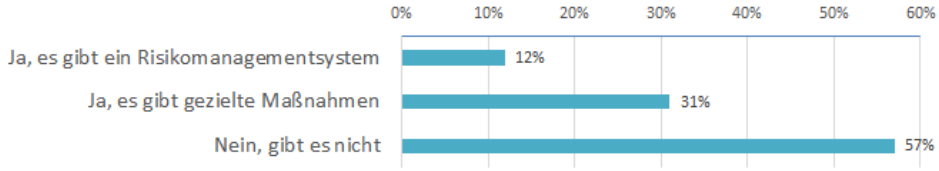

Abbildung 3.2: Risikomanagement im Einkauf der Möbelindustrie, Eigene Darstellung

Im Rahmen einer weiteren Studie gaben über 80 % der Unternehmen an, „ihr Risikomanagementsystem in den nächsten ein bis zwei Jahren auf den Prüfstand stellen zu wollen, um es kontinuierlich zu verbessern“ [LZA11]. Es lässt aus den drei Studien schließen, dass auf Grund der unterschiedlichen Ergebnisse die Risikopolitik gezielt und auch evolutionär durch die Unternehmen bestimmt wurde.

Ausgehend von der Mission und Strategie des Unternehmens und dessen Philosophie ist die Richtung der Unternehmensrisikostrategie anhand der Risikotragfähigkeit des Unternehmens individuell festzulegen. Die generelle Ausrichtung des Unternehmens bildet die Grundlage der weiteren Festlegung zur Bewältigung von Unternehmensrisiken. Anhand der festgelegten Risikopolitik werden weitere Richtlinien im Unternehmen festgelegt. Ausgangsbasis dazu bilden die Kerngeschäfts- sowie Begleitprozesse (Managementdisziplinen) mit ihrer Prozessarchitektur oder Organisationseinheit. Für jeden Prozess oder Organisation ist eine Schutzbedarfsanalyse durchzuführen wobei diese sich bei KMU im Detaillierungsgrad unterscheidet [Mül15].

Eine weiterführende Analyse zum Unternehmensrisikomanagement gehört die Portfoliotechnik. Analysen zu technologischen Entwicklungen als Konsequenz für die Produktentwicklung sind im Bezug zur Produkt- und Marktentwicklungen für KMU von wesentlicher Bedeutung um ihre Produkte am Markt auszurichten. Diese Umweltanalyse stellt eine Chancen-Risiken-Analyse dar um strategische Risiken auszuschließen. Die Marktanteils- und Marktwachstums-Analyse, entwickelt von der Boston Consulting Group, stellt den relativen Marktanteil zum Marktwachstum der eigenen Produkte dar, woraus sich „Normstrategien“ für eine ausgewogene Geschäftsstruktur ableiten lassen [Wen13]. Für KMU ist die Portfoliotechnik interessant um durch Risikostreuung mit unterschiedlichen Produkten das gesamtunternehmerische Risiko zu minimieren. Auch hier wird sich der Detaillierungsgrad

zwischen kleinen und mittleren Unternehmen unterscheiden, da kleine Unternehmen auch eine kleinere Angebotsbreite besitzen.

Eine SWOT Analyse umfasst eine Stärken-Schwächen-Analyse (Strength-Weakness) und eine Chancen-Risiko-Analyse, welche sehr oft bei der Entwicklung von Strategien und Positionierungen in KMU verwendet wird. Auf der Grundlage wird die Strategie des Unternehmen erarbeitet welche die langfristigen Ziele formuliert.

3.2 Bedarfsanalyse

Um so größer das Unternehmen, um so mehr interne und externe Prozesse sind vorhanden. Mittlere produzierende Unternehmen besitzen in der Regel, im Gegensatz zu kleinen Unternehmen, mehr Geschäftsprozesse. Anhand der Schutzbedarfsanalyse wird jeder Geschäftsprozess anhand einer Prozessablaufbeschreibung untersucht. Dabei werden unter anderem Infrastruktur (Gebäude, IT Struktur), genutzte Ressourcen (Material, Mitarbeiter), externe Rahmenbedingungen (z.B. Gesetze, Vorschriften, siehe Kapitel 2), Schnittstellen zu internen und externen Prozessen, Stakeholder (Mitarbeiter, Kunden, Lieferanten) oder das Prozessumfeld auf einen Schutzbedarf untersucht. Jeder Vorgang innerhalb eines Prozessablauf ist zu erfassen und separat auf den Geschäftseinfluss zu bewerten. Die Aufteilung der Sicherheitsanforderungen kann dabei in Klassen (separate Geschäftsprozesse, Organisationseinheiten, extern, intern) erfolgen um die Ergebnisse übersichtlich zu halten. Das daraus entstehende Schutzbedarfsportfolio oder auch Risikoportfolio genannt, dient der späteren kontinuierlichen Überwachung des Prozesses [Bra15].

Es ist so die Sicherheitsanforderung für jeden Prozess zu bestimmen, ob ausreichend Begleitprozesse installiert sind um damit das Gesamtunternehmerische Risiko zu beschränken. Eine Bedarfsanalyse kann z.B. über eine Expertenbefragung der jeweiligen Fachabteilungen erfolgen, welche detaillierte Kenntnisse für externe und interne Sicherheitsanforderungen zu einzelnen Prozess genau kennt. Weitere Möglichkeiten zur Analyse wäre die Fehler-Ursachen-Analyse, Interviews oder Brainstorming zur Nutzung internes Expertenwissen [Mul13]. Ferner ist zu bestimmen, welche minimalen Ressourcen notwendig sind, um einen Prozess aufrechterhalten. Daraus ließe sich dann eine Priorisierung für den Notbetrieb ableiten. Für jeden Vorgang innerhalb eines Prozess ist der jeweilige Schutzbedarf in einer Tabelle (Risk Register) festzuhalten.

3.2.1 Mittlere Unternehmen

In erster Linie geht es darum Kerngeschäftsprozesse zu sichern was für beide KMU relevant wäre. Für KMU ist jedoch eine Unterscheidung im Detaillierungsgrad der Bedarfsanalyse festzustellen, da mittlere Unternehmen mehr Infrastruktur besitzen und auch die Geschäftsprozesse komplexer gestaltet sind existieren auch mehr Prozesse die zu bewerten sind. Für mittlere Unternehmen gilt, sich intensiver mit ihren

	Ergebnis	Bewertung	Aufwand	Perioden
Qualitatives RM Unternehmensebene	Risikoinventar auf Stufe des Unternehmen	Qualitativ: Häufigkeit/Schadensausmaß	Workshops 1-3 h mit Geschäftsführer	jährlich
Qualitatives RM Abteilung/Prozess	Risikoinventar auf Stufe der Abteilungen/ Prozesse	Qualitativ: Häufigkeit Qantitativ: Schadensausmaß EBIT [%]	Workshops 1-3 h mit Geschäftsführer und Interne Experen	halbjährlich

Abbildung 3.3: Detaillierungsgrad des Risikomanagement bei KMU

Prozessen auseinanderzusetzen. In mittleren Unternehmen kann ein Brainstorming mit den jeweiligen Fachabteilungen stattfinden, was durch die Geschäftsführung initiiert wird und mit den Abteilungen vertieft wird (Top Down). Das bestätigt auch die Studie „Risikomanagement im Mittelstand“[LZA11], womit 32 % der befragten deutsche Unternehmen mit internen Experten sowie mit Checklisten (26 %) die Analyse durchführen.

3.2.2 Kleine Unternehmen

Generell sollten sich auch kleine Unternehmen mit Risikomanagement auseinandersetzen und ggf. erfahrenen Berater oder Unternehmer beim Aufbau Risikomanagementsystems einsetzen. Besonders am Anfang, zur Gründung eines kleinen Unternehmen ist eine Risikoanalyse je nach unternehmerischen Risiko durchzuführen um anfängliche Unternehmerische Risiken auszuschließen. Erfahrene Berater liefern das Expertenwissen zur Bewertung des Product-Life-Cycle in kleinen Unternehmen. Die Weiterentwicklung des Risikomanagement im Unternehmen erfolgt dann durch den Lernerfolg evolutionär.

KMU können mit einer wesentlichen Frage den notwendigen Schutzbedarf für Ihr Unternehmen ermitteln: In welcher internen und externen Beziehung steht mein Produkt/Dienstleistung im gesamten Product-Life-Cycle und welche Risiken können auftreten? Siehe Abbildung 3.4. Daraus lässt sich ableiten, welchen Risikomanagementbedarf ein Unternehmen, unter Berücksichtigung von Kosten-Nutzen-Aspekten, wirklich hat.

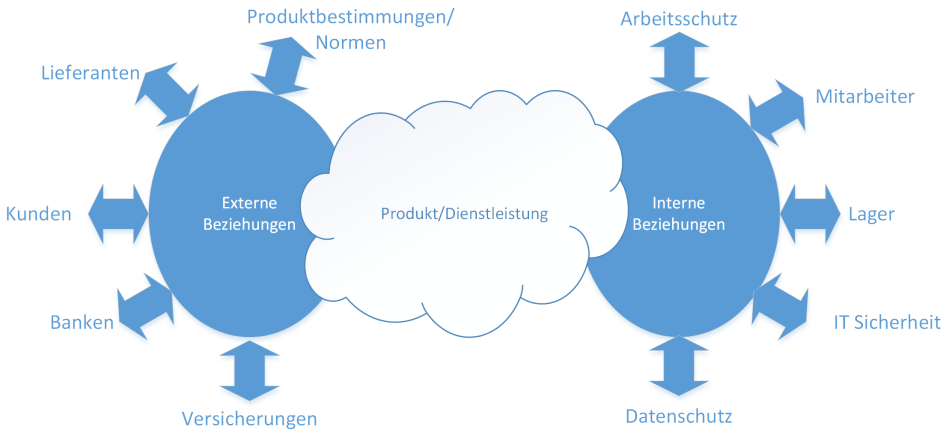

Abbildung 3.4: Produkt/Dienstleistung in Beziehung der Umwelt

3.3 Analyse der Sicherheitsanforderung

Jeder Schutzbedarf wird im Hinblick auf seine Wichtigkeit für das Unternehmen klassifiziert. Die Wichtigkeit dient der Priorisierung der weiteren Vorgehensweise im Bezug auf Kosten, da alle zusätzlichen Unternehmerischen präventiven Aktivitäten Geld kosten. Denn die Wirtschaftlichkeit des Unternehmens soll weiterhin gegeben sein.

Die möglichen Risiken müssen zuerst nach der Wichtigkeit (Wahrscheinlichkeit) und ihren Wirkungen (Auswirkung mit Schäden und Verlusten) für die Organisation beurteilt werden [Bra15]. Die Abbildung 3.5 auf Seite 16 zeigt als Beispiel den Prozess zur Vertragsvorbereitung für mittlere projektorientierte Unternehmen. Einzelne Vorgänge wurden auf ihre Wichtigkeit für das Unternehmen bewertet. Die Analyse zeigt auch, dass einzelne Prozesse weiter untersucht werden müssen, da die bisherige Bewertung nur grob durchgeführt wurde.

3.4 Implementierung

Für jedes identifiziertes Risiko ist zu entscheiden, welche Strategie, unter Berücksichtigung von Kosten-Nutzen-Aspekten, verfolgt werden soll. Mit grafischer Darstellung der einzelnen Risiken lässt sich eine Entscheidungsgrundlage, wie in Abbildung 3.6 auf Seite 17 erstellt, bilden. Die identifizierten Risiken aus allen „Risk Registern“ sind nun nach Wichtigkeit (siehe Kapitel 3.1) zu bewerten. Qualitative Bewertungen in Wahrscheinlichkeit und Auswirkung (siehe Abbildung 16) werden jetzt quantitativ analysiert um Auswirkungen auf Kosten und Termine festzustellen. Je nach Risikopolitik, sowie festgelegter Risikotragfähigkeit des Unternehmen werden die Risikoklassen (Achsenwerte 1-10 in Bild 3.6) mit einen Schadenswert belegt. So kann die Auswirkung 8-10 zum Beispiel als „existenzgefährdend“, sowie die Wahrscheinlichkeit 1-3 als „unwahrscheinlich“ qualifiziert

Risikoidentifizierung			Risikobewertung		
Risiko-gruppe	*Risikokategorie*	*Risikofaktoren*	*Wahrschein-lichkeit [1-10]*	*Auswirk-ung [1-10]*	*Strategie zur Risikobewältigung*
Vertragsvorbereitung	**Vertragspartner**	Firmierung unklar	2	5	Informationsgewinnung
		Unternehmens-Verflechtungen unklar	3	5	Bonitätsprüfung
		Branchengerüchte	2	10	Informationsgewinnung
	Liquidität	Zahlungsfähigkeit	2	9	Bonitätsprüfung
		Zahlungsziele	5	10	Genaue Angebotsformulierung
	Projekt Vorarbeiten	Sensible Kundendaten wurden weiterverwendet	3	9	Geheimhaltungsvereinbarung im Letter of Intent
		Es wurde ohne Vertragliche Grundlage Projektarbeit geleistet	4	8	Aufteilung der Vorfeldkosten im Letter of Intent
	Techn. / kaufm. Anforderungen	Spezifikationen unklar	6	9	Informations-gewinnung
		Liefermenge	4	6	Genaue Angebotsformulierung
		Lieferzeit	8	8	Genaue Angebotsformulierung
		Einsatzzweck	4	9	Genaue Angebotsformulierung
		Lieferort und Einsatzort	3	8	Genaue Angebotsformulierung
	Risikobewertung	Realisierbarkeit	6	10	- Überprüfung hinsichtlich - technischer - kaufmännischer - rechtlicher Machbarkeit
		Rentabilität	6	8	- Überprüfung hinsichtlich -finanzieller Aspekte
		Unternehmensziele/ -politik	6	6	Abgleich mit - Unternehmensethik - Haftungsbereitschaft - Strategie

Abbildung 3.5: Risikoidentifizierung

werden. Die Risikoklasse „Existenzgefährdend“ wird dann mit einem individuellen, unternehmensabhängigen Schadenswert, z.B. 100.000 Euro quantifiziert. Die Anzahl der Risikoklassen, Quantifizierungsstufen, sowie mögliche Schadenswerte werden unternehmensspezifisch angepasst.

Strategien, Standards, Richtlinien

Sind die zu bearbeitenden Risiken (Bedrohungen) ausgewählt, ist für jedes identifizierte Risiko eine entsprechende Risikostrategie (Risk Response Strategie) festzulegen. Hierfür gibt es folgenden Risikostrategien [Mul13]:

Bedrohungen

- Bedrohung vermeiden; mit entsprechenden Unternehmensregeln die Eintrittswahrscheinlichkeit vermeiden (aktive Maßnahmen)
- Bedrohung transferieren; Verantwortung verlagern, z.B. durch Versicherungen (passive Maßnahmen)
- Bedrohung mindern; Wahrscheinlichkeit des Eintreffens minimieren (aktive Maßnahmen)
- Bedrohung akzeptieren

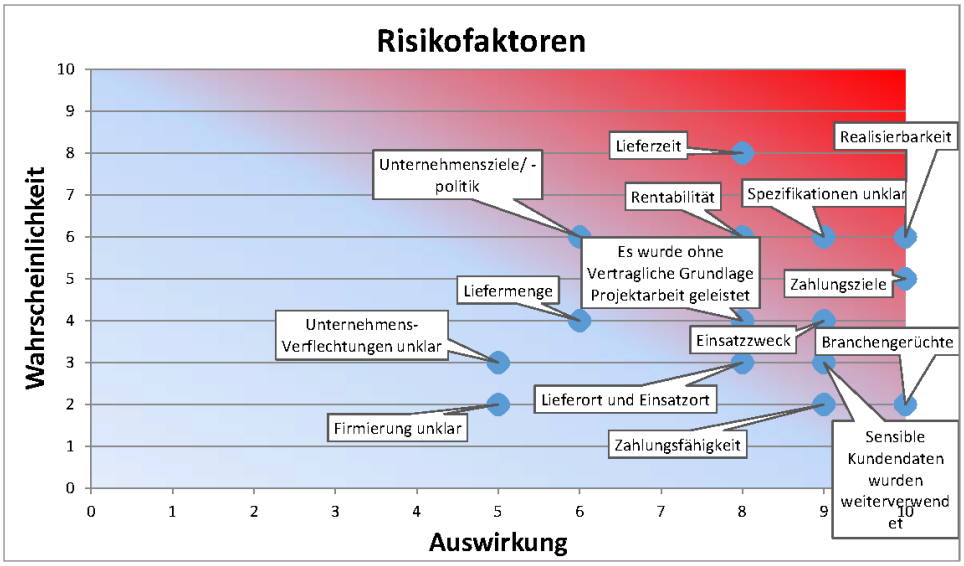

Abbildung 3.6: Risikofaktoren

Chancen

- Chance ausnutzen; sicherstellen, dass ein Ereignis eintritt (aktive Maßnahmen)
- Chance teilen; sicherstellen, dass auch andere davon Profitieren (passive Maßnahmen)
- Chance verstärken; Wahrscheinlichkeit erhöhen (aktive Maßnahmen)
- Chance akzeptieren

Begleitprozesse oder Standards werden festgelegt um Bedrohung zu vermeiden oder zu mindern, Chancen auszunutzen oder zu verstärken. Der Begleitprozess Kapazitätsmanagement beschreibt zum Beispiel welchen Durchsatz ein einzelner Prozess benötigt. Daraus lassen sich Anforderungen an der Anzahl der Arbeitsplätze oder des Raumbedarf ermitteln. Weitere Begleitprozesse sind zum Beispiel das Konfigurationsmanagement (Gebäude und Haustechnik), Arbeitsschutzmanagement, Betriebssicherheit, Finanzmanagement, Projektmanagement, Qualitätsmanagement, Changemanagement, Kapazitätsmanagement, Wartungsmanagement, Securitymanagement, Vertragsmanagement, Dokumentationsmanagement oder Personalmanagement [Mül15].

Weiterhin können Richtlinien als Risikostrategie festgelegt werden. Dazu zählen zum Beispiel Sicherheitsregeln (Einweisungspflichten, Umgang mit Daten intern/extern), Kommunikationsregeln (Informationen an Dritte), Dokumente zur Prozessbeschreibung, Regeln zur Ressourcenplanung, E-Mail/Internet-Nutzung, Regeln zu Antrags- und Genehmigungsverfahren, Datenschutzmanagement,

Richtlinien zur Zutrittskontrollsystem und vieles mehr. Diese Richtlinien wird als internes Kontrollsystem bezeichnet (IKS) [Mül15].

KMU werden nicht alle Risiken im Detail, auf Grund von Ressourcen und Finanziellen Mitteln, analysieren und umsetzen können, daher gilt für KMU zuerst nach möglichen Höchstschäden, also dem Erwartungswert für eine Schaden zu priorisieren [BEFPR15]. Für produzierend Unternehmen wäre wichtig, Produkte müssen eine entsprechend Qualität aufweisen und nach der jeweiligen Norm entsprechen um das Risiko der Produkthaftung auszuschließen (vgl. 2.2). Die Fertigung sollte mit redundanten Fertigungsmöglichkeiten ausgestattet sein um Produktionsausfälle zu vermeiden. Für Handel und Dienstleister wäre der professionelle Betrieb des Vertragsmanagements und des Zahlungsverkehrs wichtig.

Lieferanten sollten bei KMU diversifiziert werden um ein Single-Sourcing zu vermeiden (Operative Risiken), ein Bonitätsprüfung und Forderungsmanagement sollte professionell betrieben werden (Finanzielle Risiken). Die Maßnahmen dienen der Verringerung von Forderungsausfällen. Weiterhin wäre die Buchführungspflicht selbstverständlich, was den Forderungen aus GmbH-Gesetz und HGB entspricht (vgl. 2.1/2.4). Sollte das Geschäft in Richtung E-Commerce ausgelegt sein, wäre es für kleine Unternehmen sinnvoll auf professionelle Shopsysteme von extneren Anbietern zurückzugreifen um Verfügbarkeit, Missbrauch und Datensicherheit zu gewährleisten (vgl. 2.5). Weiterhin ist eine Markt Umweltanalyse mit der Portfoliotechnik von Produktentwicklungen im Bezug zur Produkt- und Marktentwicklungen für KMU von wesentlicher Bedeutung um ihre Produkte am Markt auszurichten. Diese Portfolio-Umweltanalyse stellt eine Chancen-Risiken-Analyse dar (Strategische Risiken). Diese genannten Maßnahmen dienen der Sicherung zu externen Beziehungen [Joa16].

Zu Maßnahmen zur Sicherung der internen Beziehungen kann man nachfolgende benennen: Arbeitsschutz, IT-Sicherheit, Datenschutz, Arbeitsverträge für Mitarbeiter. Hierzu empfiehlt es sich Branchenspezifisch bei Industrie- und Handelskammer Empfehlungen über die Gestaltung einzuholen. Personalrisiken können durch Nachfolgeregelung, Mitarbeiterbefragungen, Belohnungskonzepte vermindert werden um Fluktuation und den dadurch entstehenden Know-How Verlust zu verhindern. Organisatorische Maßnahmen wie Qualitäts-Sicherungsmaßnahmen durch Arbeitsanweisungen, Systematische Kontrollen durch ein fortlaufendes konsequentes Controlling (Frühwarnsystem, Siehe 3.5) gehören ebenfalls zu notwendigen internen Maßnahmen und runden den PDAC Zyklus ab [Joa16].

Nachfolgende Tabelle 3.7 gibt zusammenfassend eine Überblick über sinnvollen Risikomanagementmaßnahmen für KMU [BEFPR15]. Die Weiterentwicklung des Risikomanagement im Unternehmen erfolgt dann durch den Lernerfolg evolutionär.

Risiko Gruppe	Risiken	Maßnahme
Strategischen Risiken	Fehlinvestitionen	Portfoliotechnik, SWOT Analyse, Marktbeobachtung, Innovationsmanagement
	Beteiligungen	
	falsche Schwerpunkte in der Produktpalette	
	Standortfaktoren	
	Neuinvestitionen	
Operative Risiken	Maschinenausfälle	Diversifikation von Lieferanten, Lagerbestände reduzieren, Qualitätssicherungssystem, Vertragsmanagment
	mangelnde Produktionskapazitäten	
	Abhängigkeit von wenigen Kunden und Lieferanten	
	Lagerhaltung/Transport	
	Qualität/Norm	
	Vertragsrisiken	
Finanzielle Risiken	Liquiditätsengpässe	Reduzierung von Verbindlichkeiten, Lagerbestand reduzieren, konsequentes Controlling, Kostenträgerrechnung, Bonitätsprüfung, Forderungsmanagement
	Verweigerte Kredite	
	Kreditlinien	
Datenverarbeitung	Datenschutz IT Systeme	Passwortschutz, Zugriffsberechtigung, IT Backups, Weiterentwicklung von Software
	Datenbanksysteme	
	Verfügbarkeit	
	Missbrauch	
Regulatorische Risiken	Gesetzes- oder Normänderungen	Beratung bei IHK, Versicherungen
	Umweltschutz	
	Arbeitsrecht, Arbeitsschutz	
	Objektrisiken	
Personalrisiken	fehlende Nachfolgeregelungen	Vertreterregelung, Mitarbeiterbefragungen, Arbeitsanweisungen
	hohe Mitarbeiterfluktuation	
	Fertigungsqualität	
Datenverarbeitungsrisiken	Mail-Accounts, Phishing	IT Sicherheit extern professionell verlagern, „Vier-Augen-Prinzip“, systematischen Kontrollen
	Prozesssicherheit wichtiger Porzesse	
Politische Risiken	Veränderungen der politischen Situation	Beratung bei IHK

Abbildung 3.7: Risikoprioritäten KMU

3.5 Überprüfung

Durch ständig sich veränderte Bedingungen bei Geschäftstätigkeiten, Märkten oder Kunden unterliegt Risikomanagement einer kontinuierlichen Anpassung, Veränderung und Weiterentwicklung. Dieser Regelkreis der kontinuierlichen Planung, Ausführung, Überprüfung entspricht dem Deming- bzw. PDCA-Zyklus. Ein wichtiges Instrument zur kontinuierlichen Überwachung zur Risikoerkennung ist das interne Controlling. Sowie kontinuierliche Sicherheitsprüfungen, um zu prüfen ob in den einzelnen Prozessen das gewünschte Risikoniveau erreicht wurde. Ein Berichtswesen hat den Zweck dem Management einen regelmäßigen Überblick über die aktuelle Risikosituation des Unternehmens zu geben. Ein Berichtswesen beinhaltet die kompletten Daten unternehmerischer Tätigkeiten wie Finanzzahlen oder Kapazitätsreports [Mül15].

Kapitel 4

Zusammenfassung der Ergebnisse

Die Arbeit veranschaulicht die Gestaltung eines professionellen Risikomanagementprozesses und bewertet zugleich die erforderlichen Maßnahmen für KMU. Es wurde dabei das verarbeitende Gewerbe, der Handel sowie der Dienstleistungssektor betrachtet, da diese den größten Anteil der KMU bilden. Die Untersuchung von Anforderungen aus Gesetzen, Normen und Verordnungen in Kapitel 2 ergab, dass es kein verpflichtendes Risikomanagement für KMU gibt. Lediglich die Norm ISO 31000 beschreibt Empfehlungen zur Gestaltung für ein Risikomanagement im Plan-Do-Check-Act-Zyklus. Daraus ergibt sich, dass die Implementierung eines funktionierenden Risikomanagementprozesses im Unternehmen als eine elementare Managementaufgabe angesehen werden kann, da unentdeckte Gefahren wesentlich über das Scheitern und fortbestehen eines Unternehmens entscheiden können.

Im Kapitel 3.1 wurde Anhand von drei Studien zur Risikopolitik in deutschen Unternehmen gezeigt, dass die Risikostrategie je nach Brache unterschiedlich ausfällt, jedoch Unternehmen generell bestrebt sind ihre Wertschöpfungskette der Kerngeschäftsprozesse aufrecht zu erhalten. Weiterhin gaben 80 % der Unternehmen an, dass sie ihr Risikomanagementsystem alle zwei Jahre auf den Prüfstand stellen. Es lässt sich daraus schließen, dass die Risikostrategie in den Unternehmen gezielt bestimmt wurde und auch evolutionär angepasst wird. Das bedeutet für KMU, dass ein Risikomanagement individuell zur Mission und Strategie der Geschäftsfelder anfänglich detailliert und danach kontinuierlich zu erfolgen hat.

KMU unterscheiden sich jedoch im Detaillierungsgrad der Schutzbedarfsanalyse, da kleine Unternehmen im Gegensatz zu mittleren weniger Ressourcen und Infrastruktur besitzen und auch die Geschäftsprozesse einfacher gestaltet sind. In mittleren Unternehmen erfolgt die Risikoanalyse nach einer Studie zusammen mit dem Geschäftsführer und internen Experten (32 %) sowie durch Checklisten (26 %). Die geschäftsführende Person bei kleinen Unternehmen greift für die Analyse auf erfahrene Berater oder Unternehmer zurück. Eine sinnvolle Detaillierung und

notwendige Regelmäßigkeit zur Bedarfsanalyse wurde in Kapitel 3.3 für KMU erstellt. Für KMU wurde in dieser Arbeit eine Fragestellung entwickelt, um den Bedarf zum sinnvollen Risikomanagement für KMU zu bestimmen und so ein Konzept festzulegen: In welcher internen und externen Beziehung steht mein Produkt/Dienstleistung im gesamten Product-Life-Cycle und welche Risiken können auftreten? Daraus lässt sich für KMU, z. B. in einem Brainstorming mit internen Experten unter Berücksichtigung von Kosten-Nutzen-Aspekten ein sinnvolles zu bearbeitendes Risikoportfolio bestimmen. Die Priorisierung erfolgt bei KMU, nach möglichen Höchstschäden, es wird also der Erwartungswert für einen möglichen Schaden quantifiziert. Die Priorisierung in der weiteren Vorgehensweise ist gerade bei KMU wichtig, da alle zusätzlichen unternehmerisch-präventiven Aktivitäten, Ressourcen binden und Geld kosten. Für die quantifizierten Risiken ist eine entsprechende Risikostrategie (Risk Response Strategie) festzulegen. Für KMU wären in erster Linie wichtig, die operative Tätigkeit zu sichern. Für produzierende Unternehmen wäre das, Produkte müssen der verkauften Qualität und nach der jeweiligen Norm entsprechen, um das Risiko der Gewährleistung und Produkthaftung auszuschließen. Die Fertigung sollte mit redundanten Fertigungsmöglichkeiten ausgestattet sein, um Produktionsausfälle zu vermeiden. Für Handel und Dienstleister wäre der professionelle Betrieb des Vertragsmanagements und des Zahlungsverkehrs wichtig. Weiterhin wäre es für alle KMU wichtig Lieferanten zu diversifizieren um ein Single-Sourcing zu vermeiden (Operative Risiken), eine Bonitätsprüfung und Forderungsmanagement muss professionell betrieben werden, um Zahlungsausfälle zu vermeiden, Liquidität zu wahren und eigene Kreditlinien nicht zu gefährden (Finanzielle Risiken). Die IT-Struktur sollte professionell errichtet werden, um Verfügbarkeit, Missbrauch und Datensicherheit zu gewährleisten. Die Lagerhaltung sollte minimiert werden, um gebundenes Kapital zu verringern und das Alter der Bestände nicht zu überschreiten. Weiterhin ist die SWOT-Analyse mit der Umfeld- und Unternehmensanalyse zur Produkt- und Marktentwicklung für KMU von wesentlicher Bedeutung, um ihre Produkte am Markt auszurichten (Strategische Risiken). Diese genannten Maßnahmen dienen der Sicherung der externen Beziehungen.

Zur Sicherung der internen Beziehungen zählen Regulatorische Risiken wie Umweltschutz, Arbeitsrecht oder Arbeitsschutz. Hier ist es für KMU ratsam branchenspezifische Empfehlungen zur Gestaltung über die Industrie und Handelskammer einzuholen. Personalrisiken können durch Nachfolgeregelungen, Mitarbeiterbefragungen und Belohnungskonzepte vermindert werden, um die dadurch entstehende Fluktuation und Know-How Verlust zu verhindern. Organisatorische Maßnahmen wie Qualitäts-Sicherungsmaßnahmen (IKS) durch Arbeitsanweisungen, systematische Kontrollen durch ein fortlaufendes, konsequentes Controlling (Frühwarnsystem) gehören ebenfalls zu notwendigen, internen Maßnahmen und runden den PDCA Zyklus ab. Die Weiterentwicklung des Risikomanagement im Unternehmen erfolgt dann evolutionär durch den Lernerfolg.

Die Tabelle 3.7 auf Seite 19 fasst relevante Risikomanagementmaßnahmen für KMU zusammen.

Literaturverzeichnis

[BEFPR15] Wolfgang Becker, Robert Ebner, Daniela Fischer-Petersohn, and Marcus Ruhnau. *Projektrisikomanagement im Mittelstand*. Management und Controlling im Mittelstand. Springer Gabler, Wiesbaden, 2015.

[Bra15] Hans-Christian Brauweiler. *Risikomanagement in Unternehmen: Ein grundlegender Überblick für die Management-Praxis*. Essentials. Springer Gabler, Wiesbaden, 2015.

[Bun] Bundesministerium der Justiz und für Verbraucherschutz. HGB, BGB, ProdHaftG, UmweltHG, KWG.

[Joa16] Joachim Rupp. *Risikomanagement in KMU-Unternehmen*. 2016.

[LZA11] Löffler Hendrik, Zähres Raimund, and Augsten Tobias. *Risikomanagement im Mittelstand: Exklusive Benchmarkstudie zu Stand und Perspektiven des Risikomanagements in deutschen (Familien-)Unternehmen*. 2011.

[Mic15] Michael Stolle. Risikomanagement in Projekten: Vorlesung Projektcontrolling, 2015.

[Mul13] Rita Mulcahy. *PMP exam prep: Accelerated learning to pass PMI's PMP exam*. RMC Publ, Minnetonka, Minn., 8. ed. edition, 2013.

[Mül15] Klaus-Rainer Müller. *Handbuch Unternehmenssicherheit: Umfassendes Sicherheits-, Kontinuitäts- und Risikomanagement mit System*. Springer Vieweg, Wiesbaden, 3., aktualisierte und erweiterte auflage edition, 2015.

[Sta16] Statista. Statistiken Risikomanagement, 2016.

[Wen13] Susanne Wendt. *Strategisches Portfoliomanagement in dynamischen Technologiemärkten: Entwicklung einer Portfoliomanagement-Konzeption für TIME-Unternehmen: Univ., Diss.–Bamberg, 2012*. Unternehmensführung & Controlling. Gabler Verlag, Wiesbaden, 2013.