Zeitschrift für Controlling & Management

Controlling & Management Review

WHU
Otto Beisheim School of Management

Wie Evonik-IT seine IT-Risiken steuert

Um formale Audit-Anforderungen zu erfüllen, fokussiert sich das Risiko-Management oft auf das kleinteilige Nachhalten von Einzelrisiken. Selten wird dabei jedoch ein Wertbeitrag realisiert. Ein Projekt der IT von Evonik zeigt, wie Unternehmen das Management ihrer IT-Risiken vereinfachen und gleichzeitig den Nutzen als Steuerungsinstrument erhöhen können.

Detlef Guski, Stephan Heinelt, Klaus Röller, Philipp Klingmann

Das IT-Risiko-Management genießt häufig den Ruf, keinen wesentlichen Beitrag zum operativen Geschäftserfolg zu leisten. Meist wird es als lästige Pflicht wahrgenommen, die primär Anforderungen der Wirtschaftsprüfer oder des internen Audits erfüllen soll – zu Unrecht. Gerade in einem innovativen Chemiekonzern wie Evonik können wir mit effektivem IT-Risiko-Management teure Systemausfälle vermeiden oder Projektrisiken reduzieren. Darüber hinaus gewinnt das IT-Risiko-Management bei uns an Bedeutung, da zentrale Paradigmen der IT-Sicherheit dem Wandel durch Trends wie Digitalisierung und Vernetzung unterworfen sind. Die früher bei uns vorherrschende komplette technische Abschottung der IT-Systeme wird durch die zunehmende Vernetzung nicht aufrechtzuerhalten sein, sondern wird aus unserer Perspektive einer Strategie des Aufdeckens und Reagierens („detect and respond“) weichen. Zusätzlich beleuchten wir IT-Risiken nicht mehr vorwiegend aus technischer Sicht, sondern ganzheitlich aus der Perspektive des operativen Geschäfts. Durch diese Veränderungen und Herausforderungen gewinnt das IT-Risiko-Management an Stellenwert unter den IT-Führungsinstrumenten.

Fallstricke für eine effektive Implementierung nehmen wir in vier Bereichen wahr:

- dezentrales und kleinteiliges Vorgehen
- teilweise nicht durchgängige Verankerung in relevanten Prozessen, Rollen und Verantwortlichkeiten
- Absicherungskultur im Umgang mit Risiken
- unvollständige Verknüpfung mit der IT-Steuerung

Integrated Risk Management Approach

Die IT von Evonik setzte sich mit diesen Fallstricken auseinander und startete das Projekt „Integrated Risk Management Approach“. Als interner IT-Provider der Evonik Industries AG ist sie unternehmenseigener Lieferant von IT-Dienstleistungen („Captive Supplier“) und wird konzernweit durch den Chief Information Officer (CIO) gesteuert und auch in Personalunion geführt. Die Evonik-IT erbringt sämtliche IT-Leistungen für die weltweit mehr als 200 Standorte. Rund 800 Mitarbeiter betreuen dabei mehr als 30.000 Arbeitsplätze und mehr als 11.000 SAP-Benutzer.

Die wesentlichen Ziele des Projektes „Integrated Risk Management Approach“ waren, ein systematischeres, zentrales

IT-Risiko-Management zu etablieren, das IT-Risiko-Management noch effektiver in der Organisation zu verankern, eine Steigerung des Risikobewusstseins zu erreichen sowie eine aktivere Risikosteuerung durch das Top Management zu ermöglichen. Die wesentlichen Lösungsansätze und die damit erreichten Ergebnisse des Projekts stellen wir nachfolgend dar.

Systematisch und zentral steuern

Grundlage für die effektive Steuerung der IT-Risiken sind für uns ein systematisches, zentral koordiniertes Vorgehen in allen relevanten Prozessschritten sowie ein zentrales Risikoregister. Für die Ausgestaltung des Risiko-Managements gibt es einige nützliche Frameworks wie COSO ERM, das ISACA „Risk IT Framework", COBIT 5 sowie zahlreiche deutsche oder internationale Normen. Im Fall der Evonik-IT haben wir uns aufgrund der Fokussierung auf IT-Risiken für das COBIT Framework entschieden und unser Vorgehen daran angelehnt sowie unser Risiko-Management-Framework in **Abbildung 1** daraus abgeleitet. Zentrales Element unseres Risiko-Management-Frameworks ist der vierstufige Prozess von der Identifizierung über die Bewertung und Steuerung bis hin zum Monitoring und Reporting der IT-Risiken.

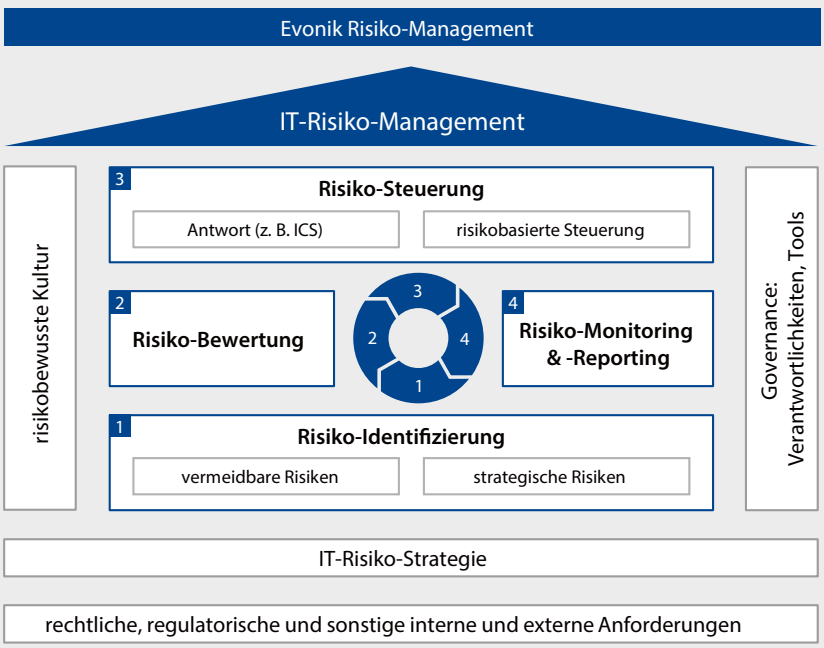
Bei der detaillierten Ausgestaltung der einzelnen Prozessschritte standen folgende Prinzipien im Vordergrund:

- Fokus auf die risikobasierte Steuerung der Top-IT-Risiken
- stärkere Verknüpfung mit dem betrieblichen Kontinuitäts-Management der Fachseite
- Einfachheit und Anwenderfreundlichkeit

Wir möchten nicht alle Risiken aktiv steuern, sondern uns auf jene Risiken beschränken, bei denen uns eine aktive Steuerung sinnvoll erscheint. Deshalb unterscheiden wir zwei von Kaplan und Mikes (2012) vorgeschlagene Kategorien von Risiken: einerseits „vermeidbare Risiken" und andererseits „strategierelevante Risiken". Ein vermeidbares Risiko könnte beispielsweise die Anwesenheit von Fenstern in den Serverräumen sein. Risiken dieser Art können wir durch definierte Vorsichts- oder Gegenmaßnahmen weitgehend vermeiden. Die Einhaltung der Maßnahmen überprüfen wir regelmäßig durch das interne Kontrollsystem. Weil uns darüber hinaus keine weitere aktive Steuerung dieser Risiken notwendig erscheint, sind sie im Weiteren nicht von Bedeutung.

Für die risikobasierte Steuerung verbleiben für uns damit die strategierelevanten Risiken, die wir nicht vollständig vermeiden können. Sie entstehen beispielsweise im Rahmen

Abb. 1 IT-Risiko-Management-Framework



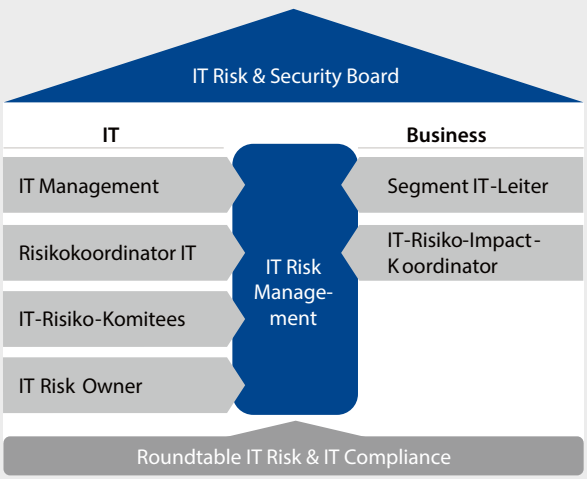
Quelle: eigene Darstellung

Zusammenfassung

- Bei Evonik hat man erkannt, dass für ein effektives Risiko-Management ein einfacher, aber strukturierter und robuster Ansatz benötigt wird.
- Das Projekt „Integrated Risk Management Approach" der Evonik-IT zeigt, wie ein solcher Ansatz implementiert und dabei die Akzeptanz unter den IT Risk Ownern sichergestellt werden kann.
- Entscheidend ist die Verknüpfung des IT-Risiko-Managements mit internen Steuerungsinstrumenten, um die Risikosituation für die strategischen Ziele der IT-Funktion transparent machen zu können.

von Projekten oder anderen Initiativen wie der Migration eines SAP-Systems oder einem größeren Technologiewechsel, also Situationen, die zu einem Ausfall von wichtigen Services führen könnten. Die entstehenden Risiken könnten wir theoretisch nur dann komplett vermeiden, wenn die zugrunde liegenden Initiativen nicht durchgeführt, damit aber auch der beabsichtigte Projektnutzen nicht erreicht würde. Strategische Risiken müssen wir daher unmittelbar gegen den Nutzen der sie hervorbringenden Initiativen abwägen. Als Ziel einer aktiven Steuerung dieser Risiken erachten wir es daher, die Risikosituation, gemessen am beabsichtigten Projekterfolg,

Abb. 2 Rollen und Gremien



Quelle: eigene Darstellung

auf ein akzeptables Niveau zu reduzieren. Ziel ist es ferner, dem CIO die Gesamtsituation der eingegangenen strategischen Risiken transparent zu machen, damit auch die Risikoexposition des gesamten Unternehmens entsprechend reduziert werden kann. Dazu führen wir ein zentrales Risikoregister ein, mit dem wir alle Informationsbedürfnisse des CIOs sowie aller weiteren Stakeholder zentral bedienen können.

Die Einschätzung des Schweregrads eines IT-Risikos nehmen wir aus Sicht der betroffenen operativen Fachbereiche vor. Der Schweregrad hängt unter anderem davon ab, welche Vorkehrungen der operative Fachbereich für den Ernstfall bereits selbst getroffen hat. Deshalb verknüpfen wir das IT-Risiko-Management innerhalb der IT mit dem betrieblichen Kontinuitäts-Management auf der Fachseite. Die IT kann die Einschätzung für die Wahrscheinlichkeit technischer Ausfälle, der Fachbereich eine Einschätzung von deren Auswirkung geben.

„Ein zentrales IT-Risikoregister ist Voraussetzung für eine Steuerung der IT-Risiken."

Durch die Verzahnung erhalten beide ein zutreffenderes Bild der Risikoexposition und können geeignetere Maßnahmen vorsehen.

Zusätzlich sind aus unserer Erfahrung die Einfachheit und Anwenderfreundlichkeit des gesamten IT-Risiko-Managements von essenzieller Bedeutung für die Akzeptanz unter den Anwendern. In der Umsetzung achteten wir daher insbesondere auf verständliche Definitionen und klar strukturierte Prozesse, die von den Akteuren aktiv gelebt werden. Dadurch, dass sich die Risiko-Eigentümer (Risk Owner) systematisch und immer wieder mit den von ihnen beeinflussbaren Risiken befassen und Verhaltensänderungen daraus ableiten, entsteht der Wertbeitrag unseres IT-Risiko-Managements für die IT-Organisation.

In Organisation und Prozessen verankern

Im nächsten Schritt verankern wir den definierten Risiko-Management-Prozess noch stärker sowohl organisatorisch als auch in den wesentlichen IT-Prozessen. In **Abbildung 2** sind die dafür definierten Rollen dargestellt. Der IT Risk Owner ist die Schlüsselfigur in unserem IT-Risiko-Management, er trägt die Verantwortung für die Identifizierung der einzelnen Risiken, die IT-Risiko-Komitees befassen sich künftig mit der Validierung der Risikosituation, und der IT-Risiko-Koordi-

nator kümmert sich um die Aufbereitung des IT-Risiko-Reportings für das IT Management. Die Hauptaufgabe des IT-Managements wiederum ist das aktive Steuern der IT-Risiken, wie das Initiieren von Gegenmaßnahmen oder die schlichte Akzeptanz von Risiken. Die Ansprechpartner auf

„Essenziell ist eine Verknüpfung der IT-Risiken mit den strategischen Zielen der IT-Funktion."

der Fachseite stellen die bereits beschriebene Verzahnung mit dem Business Continuity Management sicher. Schlussendlich wird die gesamte IT-Risikosituation vom „IT Risk & Security Board" beurteilt, einem Gremium mit Top-Management-Vertretern sowohl der Fach- als auch IT-Seite. Der „Round Table IT Risk & IT Compliance" dient hauptsächlich als Resonanzboden für die gewählten Risiko-Management-Methoden. Mit diesen Rollen und Verantwortlichkeiten vereinen wir alle notwendigen Perspektiven und stellen den notwendigen Informationsfluss sicher.

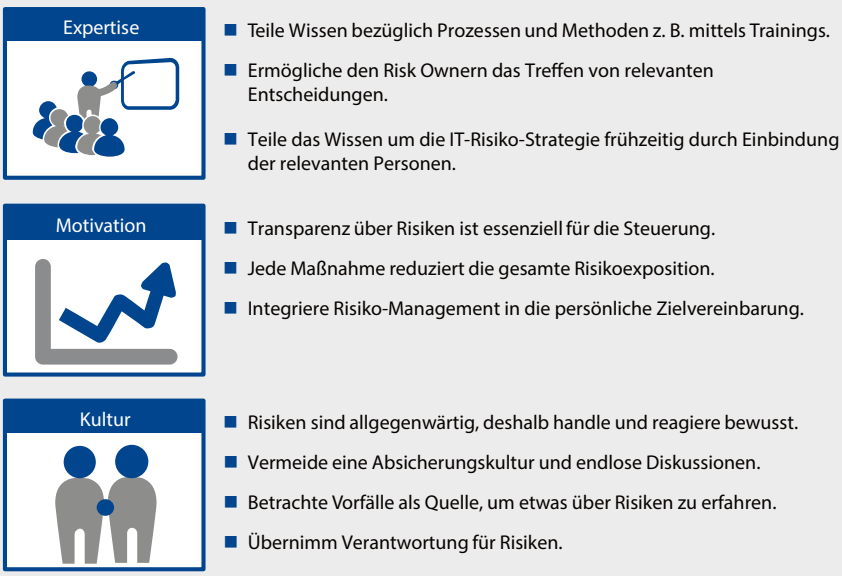
Der IT-Risiko-Management-Prozess wurde auch an einigen Stellen in der ITIL-Prozesslandschaft integriert. So fördern wir das frühzeitige Erkennen von IT-Risiken aus den risikobehafteten Initiativen heraus. Beispiele hierfür sind organisatorische Änderungen, das Service Design, kontinuierliche Service-Verbesserung oder das IT-Projekt-Management.

Risikobewusste Kultur fördern

Mit der Benennung eines IT Risk Owners für jedes Risiko haben wir eine zentrale Figur für die Identifikation und die Behandlung von Risiken eingeführt. Gerade bei den Risk Ownern möchten wir daher auch das Bewusstsein im Umgang mit Risiken weiter stärken. Das heißt jedoch nicht, dass wir eine grundsätzlich risikoaverse Haltung fördern möchten, sondern das bewusstere Treffen von Entscheidungen zur Akzeptanz oder Mitigation von Risiken. Auch stellen wir bewusst den unmittelbaren Nutzen des Risiko-Managements für die IT Risk Owner in den Vordergrund.

Dazu wurden mit den Risk Ownern, auf Ebene der Abteilungsleiter, Workshops zur Identifikation von strategischen Risiken abgehalten. Dies erlaubt gleichzeitig die Schulung des neuen Prozesses sowie die Stärkung des Risikobewusstseins. In einigen Fällen konnten direkt zusätzliche mitigierende Maßnahmen als Quick Wins abgeleitet werden, die den Nutzen des strukturierten Ansatzes direkt erlebbar machen. Ein weiterer Nutzen für die IT Risk Owner besteht darin, das Risiko-Management als Kommunikationskanal

Abb. 3 Prinzipien der Risikokultur



Quelle: eigene Darstellung

zum IT -Management zu nutzen. Vorhandene Störgefühle und Unklarheiten, beispielsweise bei großen Veränderungsprojekten innerhalb der Organisation, können sachlich als Risiko formuliert, bewertet und kommuniziert werden.

In **Abbildung 3** sind die wesentlichen kulturellen Regeln im Umgang mit Risiken nochmals dargestellt.

„Eine risikobewusste Kultur ist Voraussetzung für einen wertstiftenden Umgang mit IT-Risiken."

Top-IT-Risiken aktiv steuern

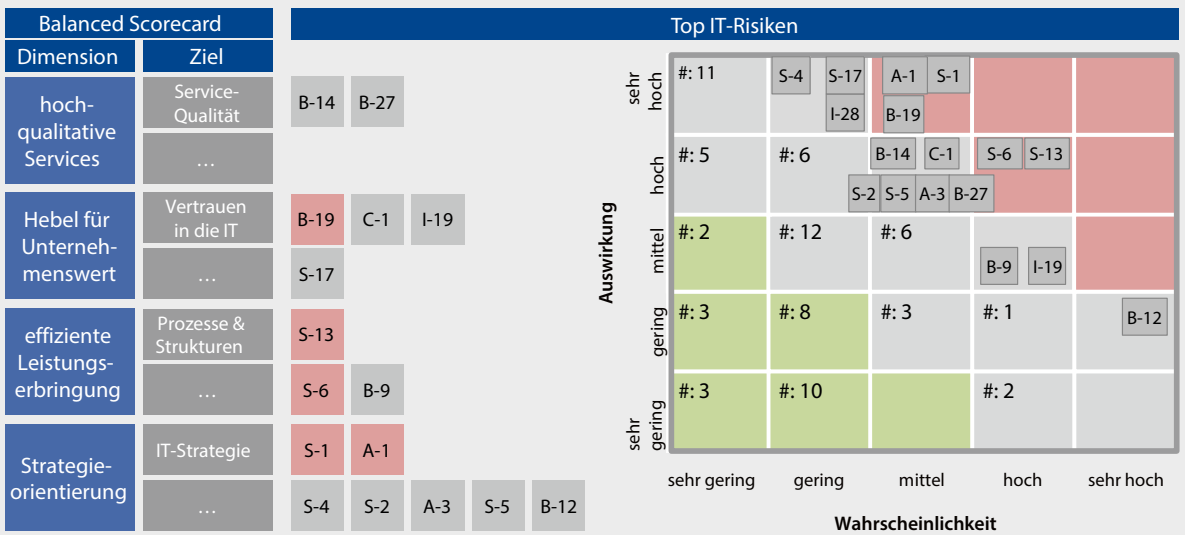
Nachdem die IT-Risiken von den IT Risk Ownern gesammelt beziehungsweise aktualisiert und mit dem Input von der Fachseite bewertet wurden, kann das Top-Management aus diesen Informationen noch besser zielgerichtete Steuerungsentscheidungen ableiten.

Kernelement der neuen risikobasierten Steuerung ist eine Verknüpfung der gesammelten IT-Risiken mit vorhandenen IT-internen Steuerungselementen. Hier ist insbesondere die IT Balanced Scorcard (BSC) zu nennen. In der Evonik-IT BSC sind die strategischen Ziele in vier Dimensionen hinterlegt. Die Dimension „hoch-qualitative Services" zielt auf die messbare Qualität der bereitgestellten IT-Services ab, „Hebel für Unternehmenswert" zeigt den Wertbeitrag der IT aus Kundensicht, „effiziente Leistungserbringung" bezieht sich auf die internen Prozesse der IT und „Strategieorientierung" auf konsequente Strategieumsetzung und künftige IT-Themen von strategischer Bedeutung. Der entscheidende Beitrag zur Steuerung unseres neu eingeführten IT-Risiko-Managements basiert auf der Berichterstattung der IT-Risiken in eben diesen Dimensionen und Zielen. Durch diese Verknüpfung sind Risiken für die aktuellen strategischen Ziele jederzeit transparent und das IT-Management kann die Bedeutung der Ziele und den Zielerreichungsgrad in die Ableitung adäquater Gegenmaßnahmen einfließen lassen. Das Steuerungsinstrumentarium der IT-Funktion wurde weiter vervollständigt und hebt die Steuerung mittels einer BSC auf ein neues Level. Eine schematische Darstellung für ein solches Reporting der Top-IT-Risiken ist in **Abbildung 4** dargestellt.

Schlussbetrachtung

Die im vorliegenden Beispiel skizzierten Ansätze für die Umsetzung und Optimierung eines IT-Risiko-Management-

Abb. 4 Risiko-Reporting in den Balanced-Scorecard-Dimensionen



B, C, S, I, A: Organisationseinheit

Quelle: eigene Darstellung

Systems haben dazu beigetragen, die Steuerung der IT-Funktion wesentlich zu verbessern. Mit der Verknüpfung des IT-Risiko-Managements mit bereits existierenden internen Steuerungsinstrumenten wie der IT Balanced Scorecard wurde eine direkte Verknüpfung der IT-Risiken mit den Zielen der IT erreicht. Dadurch wird eine Kommunikation über IT-Risiken auf einer aggregierten Ebene möglich. Dies ist ein wesentlicher Fortschritt im Vergleich zum bisherigen Risiko-Management-System, das sich stark auf die Einzelrisiken fokussierte und eine weniger managementrelevante Sicht auf die IT-Risiken erlaubte.

Handlungsempfehlungen

- Schaffen Sie Transparenz über Risiken, die auf strategische Ziele der IT-Funktion wirken.
- Machen Sie den Risk Ownern ihren konkreten Nutzen am Risiko-Management deutlich.
- Wählen Sie einen einfachen, aber strukturierten Ansatz und stellen Sie die Vollständigkeit des zentralen Risikoregisters sicher.
- Starten Sie die Implementierung und erstmalige Sammlung der strategischen Ziele top-down, beispielsweise in Workshops mit dem Management.

Literatur

Forrester Consulting (2013, September): The Business Technology Value Scorecard, commissioned by the Technology Business Management Council.

Kaplan, R. S./Mikes, A.: Managing Risks (2012): A New Framework, in: Harvard Business Review, 90 (6), p. 48-60.

Angaben zu den Autoren:

Detlef Guski
ist Director IT-Risk & IT-Quality Management
bei Evonik Industries AG,
Frankfurt am Main, Deutschland.
E-Mail: detlef.guski@evonik.com

Stephan Heinelt
ist Vice President IT Service Management
bei Evonik Industries AG,
Frankfurt am Main, Deutschland.
E-Mail: stephan.heinelt@evonik.com

Dr. Klaus Röller
ist Projektleiter bei CTcon
Management Consultants
München, Deutschland.
E-Mail: k.roeller@ctcon.de

Philipp Klingmann
ist Partner bei CTcon
Management Consultants,
München, Deutschland.
E-Mail: p.klingmann@ctcon.de