Stefan Luckhaus

Risiken in der IT:
Erkennen - Steuern - Verbessern

Ein Modell für effektives Risikomanagement in Entwicklung und Betrieb

tredition

Druck und Distribution im Auftrag des Autors:
tredition GmbH, Halenreie 40-44, 22359 Hamburg, Deutschland

ISBN
Softcover 978-3-746-90252-4
Hardcover 978-3-746-90253-1
E-Book 978-3-746-90254-8

Inhaltsverzeichnis

Einleitung

Auch für IT-Projekte gilt: Die Zukunft ist nicht festgelegt. Möchten wir einen bestimmten Zustand in der Zukunft (ein Ziel) erreichen, werden wir meist mit so vielen Einflüssen auf unserem zielführenden Weg konfrontiert, dass wir sie weder zählen noch überschauen können. Wir mögen uns treiben lassen von diesen Einflüssen, wir können sie aber auch analysieren und im Sinne der Zielerreichung störende von begünstigenden Einflüssen unterscheiden. Dies befähigt uns, die Auswirkungen störender Einflüsse (im Kontext dieses Buches als Bedrohungen oder Risiken bezeichnet) zu mindern oder ganz zu vermeiden und demgegenüber die Auswirkungen begünstigender Einflüsse (im weiteren Verlauf: Chancen) zu fördern.

Abbildung 1 zeigt in plakativer und an Alltagserfahrungen angelehnter Form, wie unterschiedliche Einflüsse den Weg zu einem Ziel, in diesem Beispiel die Einhaltung eines vereinbarten Liefertermins, beeinflussen können. Werden diese Einflüsse nicht erkannt und wird ihnen nicht gegengesteuert, führen sie zu einer Abweichung vom geplanten direkten Weg. Im schlimmsten Fall wird das Ziel nicht erreicht.

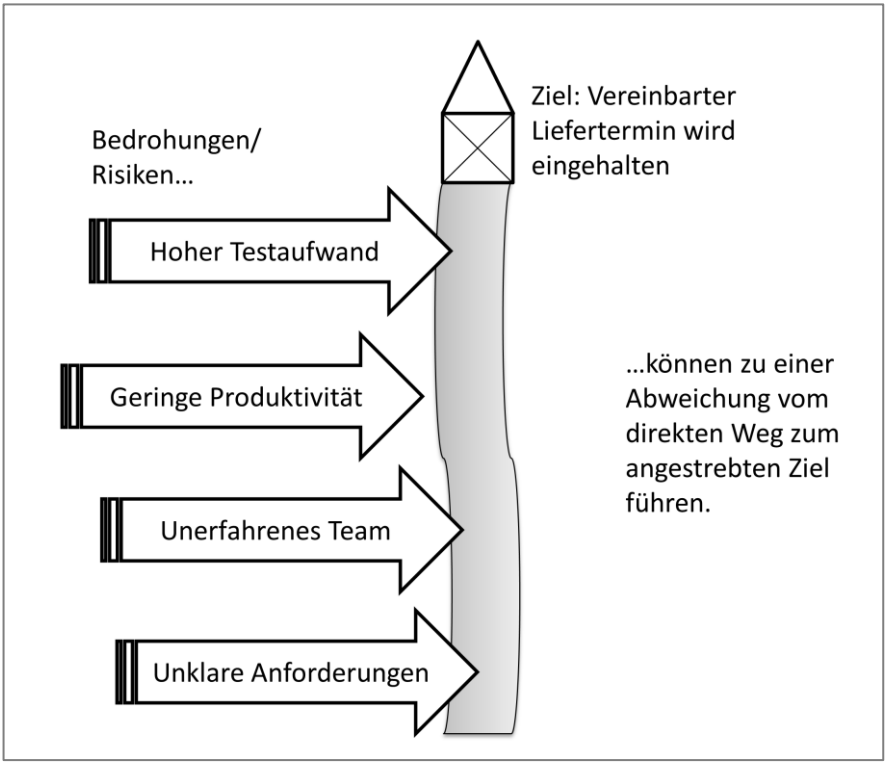

Abbildung 1: Beispiel für Einflussgrößen einer Zielerreichung

Dieses einfache Prinzip findet man in vielen modernen Managementsystemen wieder. Sie zeigen dem Management in einem bestimmten Kontext Ziele und Wege. Dabei stehen die Wege sinnbildlich für bewährte Methoden zur Zielerreichung mit zugehörigen Steuer- und Kontrollmechanismen.

In modernen Managementsystemen ist die Analyse von Chancen und Risiken ein Kernprozess und wichtiger Input zur Steuerung der Zielerreichung. Jede Unternehmensführung basiert auf einem Managementsystem und orientiert sich somit an Chancen und Risiken, ebenso beispielsweise Organisationen zur Durchführung von IT-Projekten, deren Managemen-

tsysteme sich meist an bewährten Vorgehensmodellen orientieren. Weitere Einsatzgebiete sind themenbezogene, standardisierte Managementsysteme wie beispielsweise

- Qualitätsmanagementsysteme nach DIN EN ISO 9001 [DIN EN ISO 9001 2015],
- Informationssicherheitsmanagementsysteme nach ISO/IEC 27001 [ISO/IEC 27001 2015] und
- Umweltmanagementsysteme nach ISO 14001 [ISO/IEC 14001 2015].

Dieses Buch beschreibt ein Modell für das Management von Chancen und Risiken, wie es in allen risikoorientierten Managementsystemen eingesetzt werden kann. Dabei basiert es auf praktischen Erfahrungen aus den Bereichen Softwareentwicklung und IT-Betrieb, dürfte jedoch auch auf andere Branchen übertragbar sein.

Da es im Kontext des Risikomanagements viele Begriffe gibt, die in der Praxis mit unterschiedlicher Bedeutung verwendet werden, enthält dieses Buch ein Glossar, in dem die im Buch verwendeten Definitionen dieser Begriffe angegeben sind. Im nachfolgenden Text des Buches sind Begriffe immer dann, wenn zum Verständnis die im Glossar angegebene Definition von Bedeutung ist und sie zum ersten Mal in einem Kapitel verwendet werden, gestrichelt unterstrichen.

Verweise auf weiterführende Literatur sind in eckigen Klammern angegeben und werden im Literaturverzeichnis präzisiert.

Ein Modell zum Management von Chancen und Risiken

Risikomanagement ist ein Kernprozess vieler Managementsysteme. Dabei wird diese Bezeichnung oft unter Vernachlässigung des Begriffs Chancen synonym für das Management von Chancen und Risiken verwendet. In der Hauptsache geht es bei einem solchen Prozess nicht um ein passendes Tool, sondern darum, das Zusammenspiel von Rollen, Prozessen und Methoden wie auch angemessenen Steuerungs- und Kontrollmechanismen festzulegen und diese zu etablieren. Abbildung 2 zeigt das schematische Diagramm eines einfachen und in der Praxis bewährten Modells zum Risikomanagement.

Das Dach des als Haus dargestellten Modells bilden die nachfolgend beschriebenen drei Managementebenen einer Organisation [Bleicher 2017].

- **Normatives Management:** Die sogenannte oberste Leitung, durch die Grundsätze, Richtlinien, Leitlinien und Standards festgelegt werden.
- Das **Strategische Management** ist für die Entwicklung und Planung von Vorgehensweisen zuständig, um die Vorgaben des normativen Managements zu erfüllen.
- Das **Operative Management** ist für die praktische Umsetzung der vom Strategischen Management geplanten Vorgehensweisen verantwortlich.

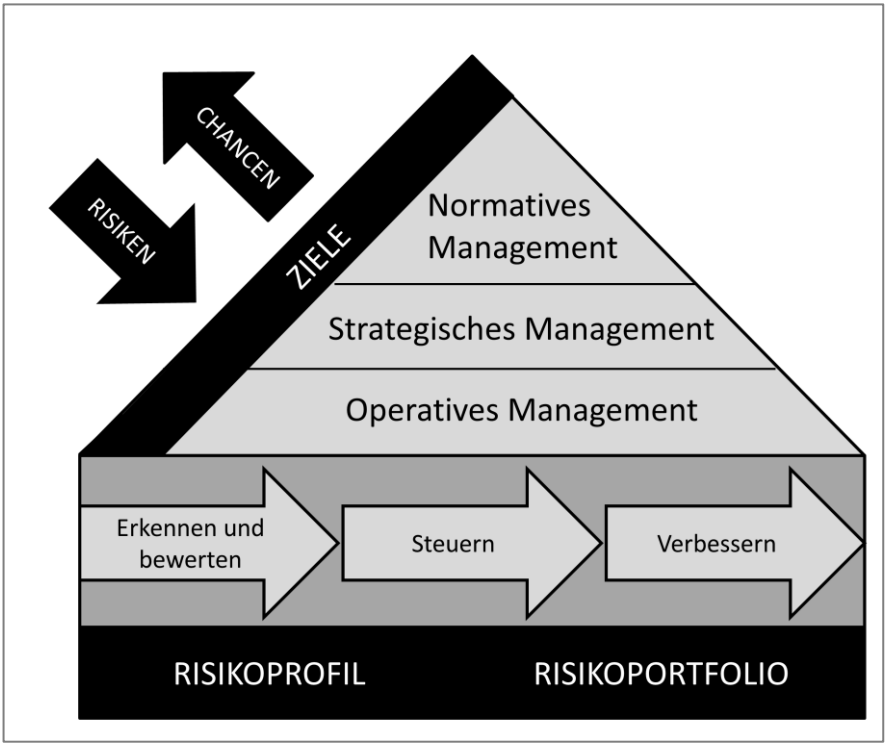

Abbildung 2: Modell zum Management von Chancen und Risiken

Die Organisation und somit alle Managementebenen werden von den gleichen Zielen getrieben, die wiederum den unterschiedlichsten Einflüssen – Chancen und Risiken – ausgesetzt sind. Je nach Kontext können dies Unternehmensziele oder auch Ziele sein, die mit einem Projekt verfolgt werden.

Unter der Leitung des Operativen Managements werden diese auf die Ziele wirkenden Chancen und Risiken im Rahmen einer Analyse erkannt und bewertet und anschließend mit Hilfe geeigneter Maßnahmen gesteuert. Angestoßen durch eine Nachbetrachtung, werden möglichst nachhaltige Verbesserungsmaßnahmen identifiziert und ihre Umsetzung, soweit

dies ökonomisch sinnvoll und möglich ist, auf den Weg gebracht. Der gesamte Prozess beginnt wieder von vorne und wiederholt sich in regelmäßigen Zyklen.

In diesem Modell stellt das Risikoportfolio die Grundgesamtheit aller Chancen und Risiken hinsichtlich der betrachteten Ziele der Organisation oder eines Vorhabens dar. Demgegenüber ist das Risikoprofil eine Auswahl genau jener Chancen und Risiken, deren Bewertung risikomindernde Maßnahmen oder eine explizite Akzeptanz der Restrisiken durch das Management erforderlich machen. Das Risikoprofil kann in jedem Zyklus erweitert oder reduziert werden und ist immer eine Teilmenge des Risikoportfolios.

Jeder neue Zyklus beginnt zunächst mit der Festlegung von für das IT-Vorhaben wesentlichen Zielen bzw. einer Nachbetrachtung bereits getroffener Festlegungen, anschließend der Identifikation von Einflussgrößen, welche die Zielerreichung bedrohen oder auch begünstigen sowie deren Bewertung bzw. Neubewertung. Mit diesem Prozessschritt „Erkennen und bewerten“ beschäftigt sich das folgende Kapitel im Detail.

Risiken erkennen und bewerten

Identifizierung spezifischer Ziele

In der Praxis lassen sich nicht alle möglichen Einflüsse auf ein IT-Vorhaben, beispielsweise ein Entwicklungsprojekt oder den Betrieb eines IT-Systems, permanent kontrollieren. Um Kontrollaktivitäten auf das Wesentliche einschränken zu können ist es zwingend erforderlich, die Ziele zu kennen, die mit dem Vorhaben verfolgt werden. Bei größeren Vorhaben ist das Management von Chancen und Risiken in der Regel nur dann ökonomisch machbar, wenn es sich auf möglichst wenig Ziele fokussieren lässt.

Ziele, die mit einem IT-Vorhaben verfolgt werden, lassen sich häufig in die folgenden allgemeinen Kategorien einordnen:

- Zeit, genauer die Einhaltung vereinbarter Termine
- die Einhaltung eines Budgets oder die Erfüllung konkreter Gewinnerwartungen
- Qualität, genauer die Einhaltung bestimmter Qualitätsmerkmale

Dabei ist die Betrachtung eines Oberbegriffs wie Zeit, Budgeteinhaltung oder Qualität in der Praxis ein zu pauschales Ziel. Termine lassen sich datieren, Gewinnerwartungen quantifizieren. Qualität kann in einzelne Qualitätsmerkmale unterteilt werden. Eine praxisnahe Orientierung für statische Eigenschaften eines IT-Systems (die Produktqualität) wie auch für Aspekte seiner Nutzung (die Nutzungsqualität) gibt die Norm ISO/IEC 25010 [ISO/IEC 25010 2011]. Die verschiedenen in der Norm definierten Qualitätsmerkmale eines IT-Systems

sind, ergänzt um zusätzliche Merkmale der Prozess- und der Dienstleistungsqualität, in den Abbildungen 3 bis 5 dargestellt – ohne Anspruch auf Vollständigkeit. Jedes dieser Merkmale kann ein Ziel sein, das mit einem IT-Vorhaben verfolgt wird und eine so große Bedeutung hat, dass Einflüsse auf die Zielerreichung einer besonderen Kontrolle unterzogen werden müssen.

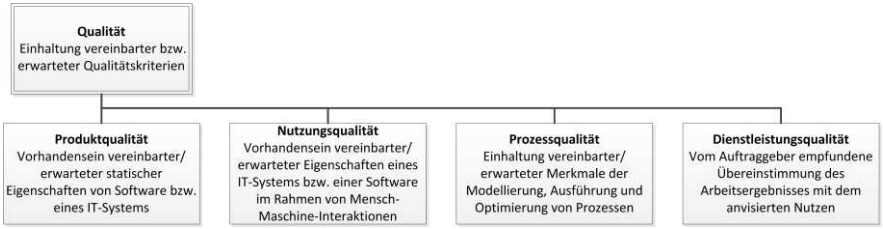

Abbildung 3: Qualitätsmerkmale (Top-Level)

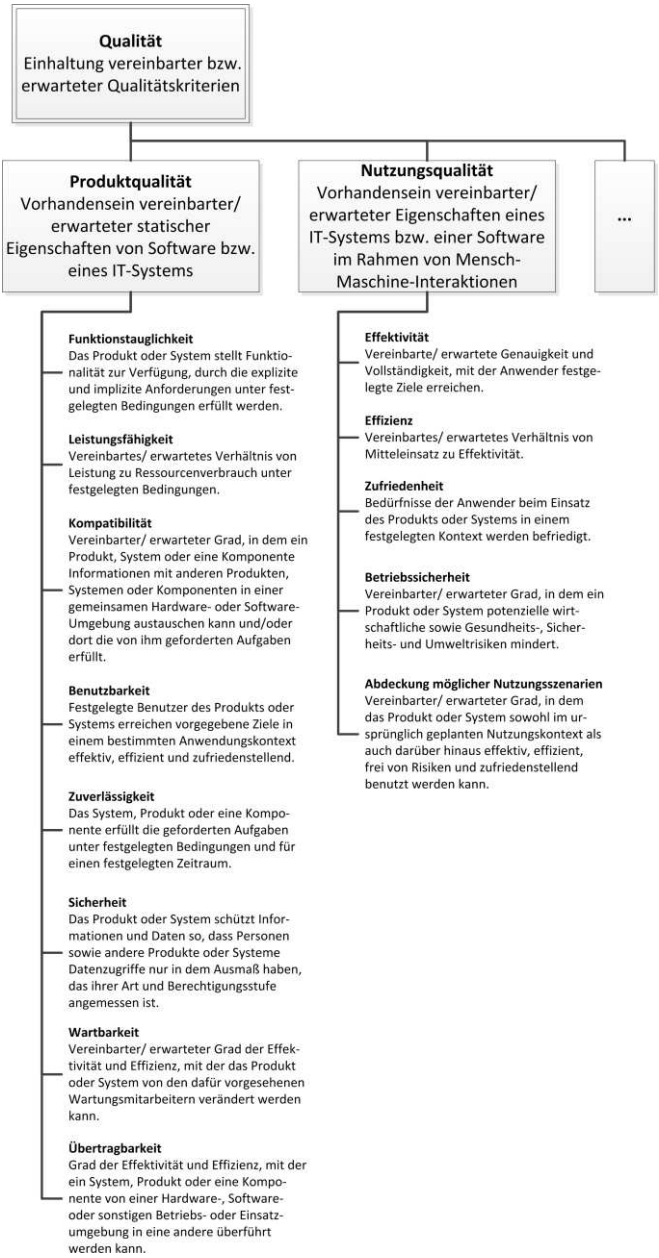

Abbildung 4: Qualitätsmerkmale und Untermerkmale (Teil 1)