

# **IT-Risiken im Griff – Neue Herausforderungen für das IT-Management**

**Lars Eisenblatt  
coniatos IT-Management Beratung AG  
Wiesbaden**

---

**Schlüsselworte: IT-Management, Risikomanagement, COBIT, Standards**

## **Einleitung**

Eine der neuen Herausforderungen des IT-Managements ist das Erkennen und Beherrschen von IT-Risiken, wie z. B. Fehlfunktion von Prozessen und Systemen oder der unberechtigte Zugriff und Diebstahl sensibler Daten. Durch pro-aktiven Umgang mit IT-Risiken können Sie die Marktposition oder sogar die Existenz Ihres Unternehmens nachhaltig sichern und die Kosten kontrollieren.

---

## Definition des Begriffs Risiko

Der Begriff Risiko hat verschiedene Aspekte, unter die man betrachten sollte.

- Aus Sicht des Managements ...  
ist ein Risiko ein unsicheres Ereignis mit negativen Auswirkungen, aber auch eine „Chance“. Denn es gilt: „kein Geschäftserfolg ohne Risiko“.
- Aus Sicht der Wissenschaft/der Mathematik ...  
ist ein Risiko folgendermaßen definiert:  
**Risiko = Eintrittswahrscheinlichkeit mal Auswirkungen**  
Ein Risiko wird zu einem Problem, sobald die Eintrittswahrscheinlichkeit = 1 ist. Somit ist ein Risiko die kalkulierte Prognose eines möglichen Schadens bzw. Verlustes im negativen Fall (Gefahr).
- Aus Sicht eines Sicherheitsexperten ...  
ist ein Risiko die negative Auswirkung der Ausnutzung einer Schwachstelle unter Berücksichtigung der Auswirkungen und der Eintrittswahrscheinlichkeit.

## Ziele des IT-Risikomanagements

Risikomanagement ist in verschiedenen Bereichen und Branchen lange bekannt. So nutzen Finanzdienstleister, wie Banken und Versicherungen, Risikomanagement zur Erbringung Ihrer Geschäftsziele. Dort ist Risikomanagement bereits gesetzlich vorgeschrieben und somit Bestandteil der Compliance. Die Betrachtung im Rahmen des IT-Managements bezieht sich meist auf die folgenden Ziele:

- Erfolgreiches Einhalten von SLA's
- Bessere Sicherung der IT-Systeme
- Bessere Risikoinformation und Beurteilung im Rahmen der IT-Budgetplanung
- Unterstützung der IT-Auswahl und des IT-Lifecyclemanagements
- Identifizieren potenzieller Probleme, bevor sie auftreten
- Planung von Maßnahmen zur Behandlung dieser Risiken

Ziel ist es dabei, die Risiken zu kontrollieren, nicht sie zwangsweise zu vermeiden. Ein Risiko lässt sich z. B. im Bereich Versicherungen nie ausschließen, denn Versicherungen leben davon, Risiken zu beurteilen und zu bewerten. Sie orientieren sich dabei an der Eintrittswahrscheinlichkeit und deren Folgen und nicht an der Behandlung der resultierenden Probleme. Durch Aktivitäten bei Erkennung des Risikos soll das Auswachsen eines Risikos zu einem Problem vermieden werden.

## Risikomanagement-Prozess

Der Risikomanagement-Prozess setzt sich aus folgenden Stufen zusammen:

1. Risikoerhebung
2. Identifizieren von Risiken und Schwachstellen
3. Bewerten der Risiken
4. Reduzierung der Risiken auf ein akzeptables Level durch Kontrollen
5. Verfolgung der Risiken und deren Auftreten

Der Risikomanagement-Prozess benötigt eine zyklische Vorgehensweise, da nicht alle Risiken sofort und endgültig eliminierbar sind. In Abbildung 1 finden Sie ein Beispiel aus dem *System Lifecycle Management*.

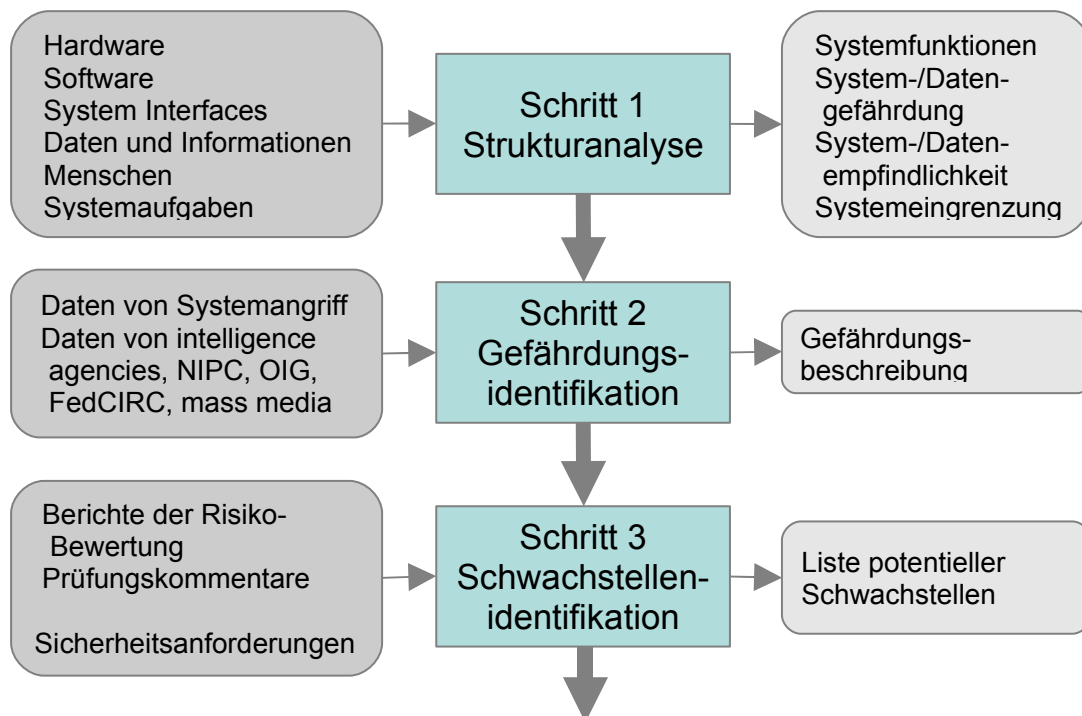
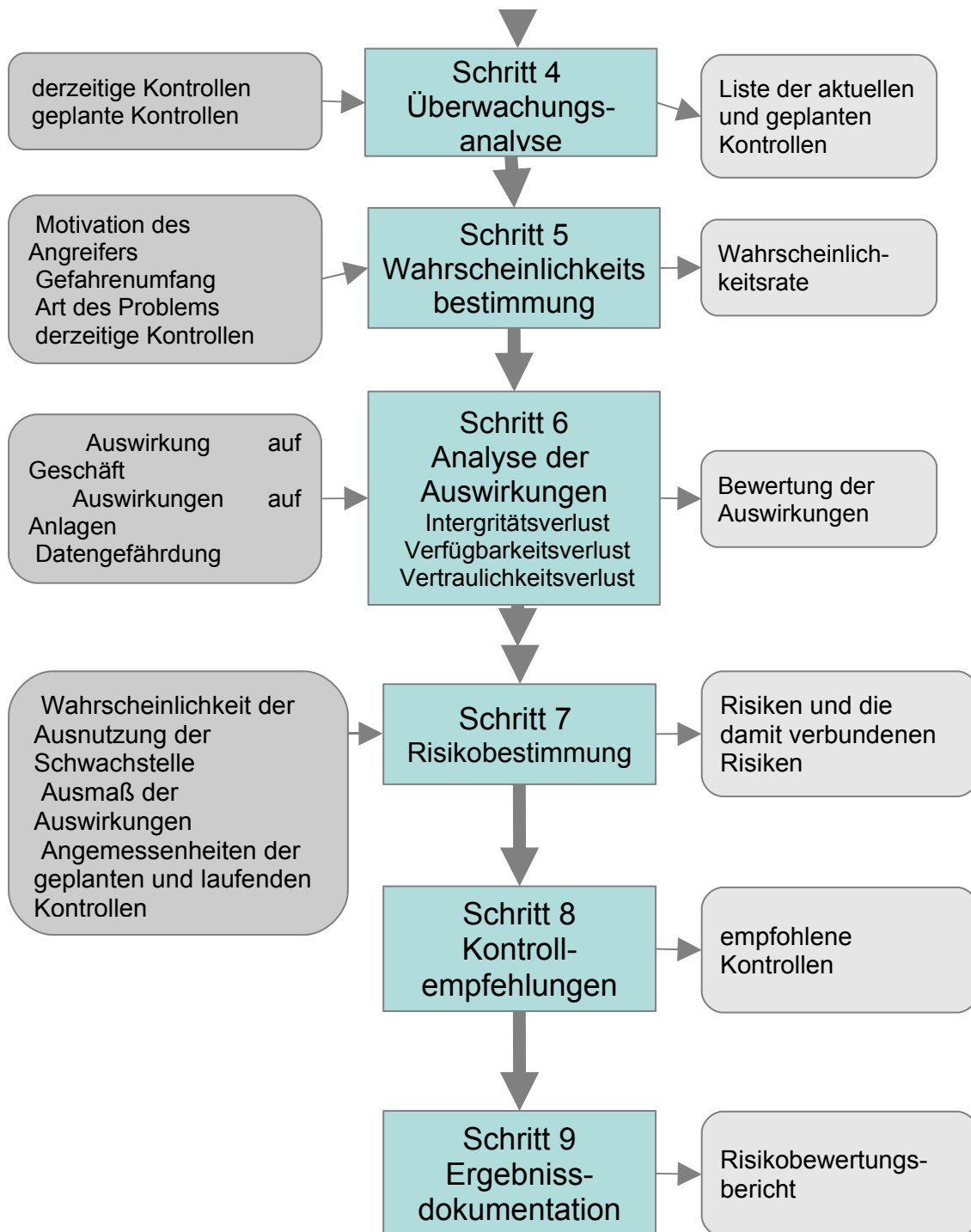


Abb. 1: Risikoerhebung



## **Risikominderung**

Die Risiken, die man in der Erhebungsphase identifiziert und bewertet hat, sollen nun gemindert werden. Es ergeben sich verschiedene Handlungsalternativen:

- **Übernehmen des Risikos:**  
Das potentielle Risiko wird eventuell durch zusätzliche Kontrollen abgemildert und letztendlich akzeptiert.
- **Vermeiden des Risikos:**  
Die Risikoursache und/oder die Risikowirkungen werden beseitigt, beispielsweise durch Deaktivieren des Systems oder des Prozesses
- **Das Begrenzen des Risikos:**  
Zusätzlichen Kontrollen werden zur Limitierung der Auswirkungen eingeführt, z. B. Intrusion Detection Systeme, Vier Augenprinzip, Separierungsschleuse oder Ähnliches.
- **Planen der Risiken:**  
Ein Risikominderungsplans mit priorisierter Implementierung der Kontrollen wird entwickelt
- **Durch eigene Forschung bzw. eigenen Aufwand Beseitigung der Schwachstelle durch einen Fix**
- **Ersatz von Risiken:** Risiken werden beispielsweise auf andere übertragen, z. B. Versicherungen, Sub-Contractors, Out-Sourcing

Bei allen Maßnahmen ist es wichtig, die Relation zwischen Aufwand und Ertrag der Maßnahmen zu berücksichtigen. Deshalb ist eine quantitative Analyse der Maßnahmen in Relation zur quantitativen Analyse der Risiken zu setzen. Die Bewertung nicht quantitativ messbarer Risiken muss Mithilfe des Unternehmens bzw. einer IT-Strategie erfolgen.

## **Risikomanagement Performance**

Grundsätzlich gilt im Risikomanagement, dass es kein unvorhersehbares Risiko gibt. Es gibt nur nicht vorhergesehene Risiken. Um wirksames Risikomanagement zu betreiben, muss die Performance des Risikomanagements bewertet werden. Dazu bieten sich verschiedene Key Performance Indikatoren an, z. B.:

- **Ausnutzung von Schwachstellen**
  - Es sind bereits erhobene Risiken zum Tragen gekommen
    - richtig / falsch gemindert
    - akzeptiert
  - Es sind bisher unbekannte Risiken zum Tragen gekommen
    - Weshalb waren die Risiken unbekannt/unbetrachtet?
  - Schadensbemessung

Diese Performance Indikatoren dienen als wichtiges Feedback für den den Verbesserungsprozess des Risikomanagements.

## **Erfolgreiches Risikomanagement durch Verankerung in der Firmenkultur**

Wichtige Grundvoraussetzung für erfolgreiches Risikomanagement ist eine entsprechende Kultur im Unternehmen. Wichtige Bestandteile dieser Kultur des Risikobewusstseins und Risikomanagements ist eine offene Kommunikation über Risiken und Budgets bzgl. Zeit und Kosten für Risikomanagement. Insbesondere wichtig ist, dass Risikomanagement keine Aufgabe einer einzelnen Person ist, sondern von allen gelebt wird. Nur dann können viele Seiten eines Systems betrachtet und viele Risiken erfasst werden. Die Erkennung von Risiken darf nicht bestraft werden, sondern muss auf allen Ebenen belohnt werden. Es muss einen definierten „Risk-Acceptance“-Prozess geben, der Widersprüche löst.

## **Verankerung von Risikomanagement in IT-Standards**

Wie bereits festgestellt, muss Risikomanagement in den Prozessen der IT verankert werden. Viele Standards finden im heutigen IT-Management bereits Anwendung. Viele Standards oder auch Best-Practices werden oder sind bereits ergänzt um Risikomanagement-Komponenten.

## BSI

Das IT-Grundschutzhandbuch des BSI ist ein weitverbreitetes Regelwerk. Es stellt die Grundlage für Informationssicherheit dar und wird vom Bundesamt für Informationssicherheit herausgegeben. In Ergänzung wurde „Risikoanalyse auf Basis von IT-Grundschutz: BSI Standard 100-3/V2.5 Mai 2008“ herausgegeben.

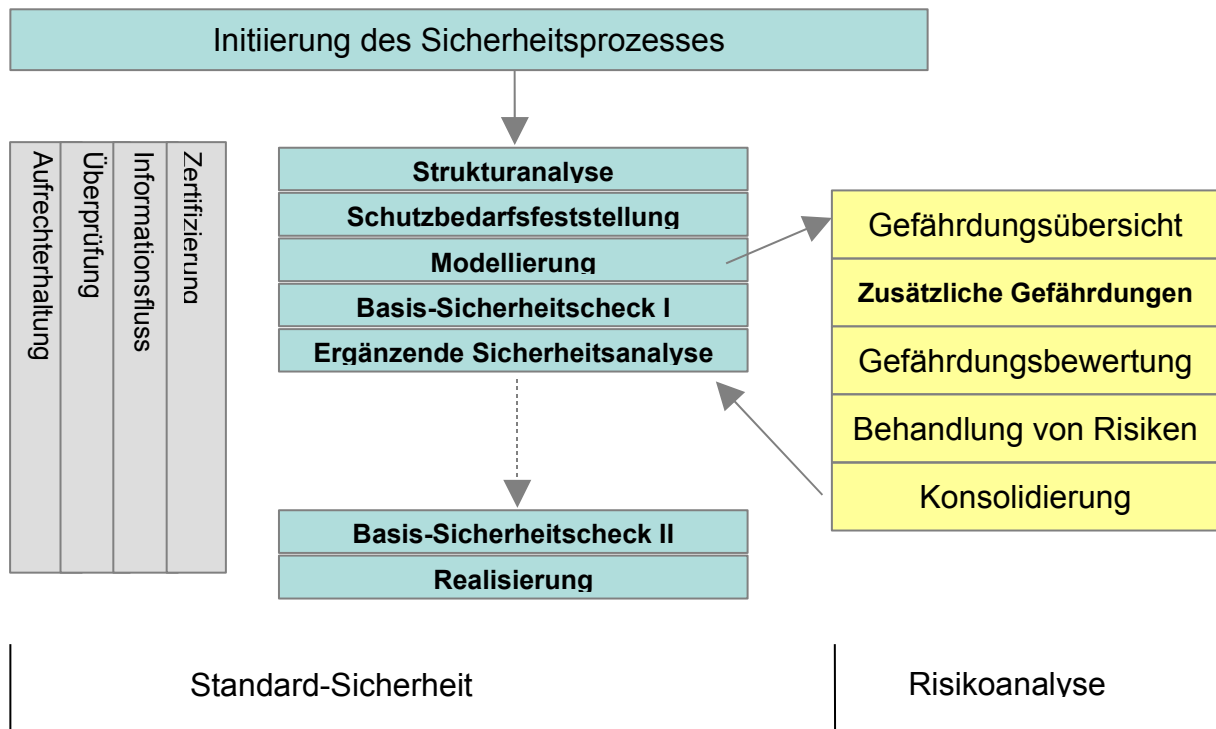


Abb. 2: Risikoanalyse im IT-Grundschutz.

## COBIT

Risikomanagement ist ein wichtiger Teilprozess in COBIT 4. COBIT ist ein Steuerungsframework für IT-Governance und wird seit 1996 von ISACA, dem Berufsverband der IT-Revisoren, herausgegeben.

IT-Governance ist die Verantwortung von Führungskräften und Aufsichtsräten und besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die Unternehmens-IT dazu beiträgt, die Organisationsstrategie und -ziele zu erreichen und zu erweitern. Die Prozessorientierung von COBIT wird durch das Prozessmodell dargestellt, welches die IT in 34 Prozesse untergliedert und in Planung, Entwicklung, Betrieb und Monitoring strukturiert. Dadurch wird eine ganzheitliche Sicht auf die IT etabliert.

Unternehmensweite Architekturmodelle helfen dabei, die wesentlichen Ressourcen für den Prozesserfolg zu identifizieren, z. B. Anwendungen, Informationen, Infrastruktur und Personal.

Der Prozess PO9 (Plan and Organize) aus COBIT 4.1 beschreibt das Risikomanagement. Er bezieht sich dabei weniger auf technische als auf organisatorische Risiken in der IT.

---