

Whitepaper: IT Risk Management by ICB

IT Risk Management

1. Investitionen in IT Risk Management machen sich bezahlt

Kaum ein Tag vergeht, ohne dass gravierende Vorfälle in Unternehmen weltweit durch die Nutzung von Informationstechnologie ans Tageslicht kommen. Durch die zunehmende Durchdringung der Geschäftsprozesse mit Informationstechnologie steigt auch das unternehmerische Risiko durch Ausfälle, Missbrauch oder Sabotage. Gesetzliche Bestimmungen und die Erfüllung der Sicherheits- und Datenschutzbestimmungen nehmen die IT-Verantwortlichen zunehmend in die Pflicht, sich mit dem IT Risk Management auseinanderzusetzen.

Vielfältige Pflichten gilt es in einer äußerst komplexen IT-Landschaft zu bewältigen. Die Erfüllung von Compliances, die Einhaltung von Datenschutz- und Datensicherheitsrichtlinien und schließlich auch die richtige Balance zwischen Chancen und Risiken zu finden, um daraus kluge Investitionsentscheidungen zu treffen.

Dem IT Risk Management kommt bei der Bewältigung dieser Vielfalt von Aufgaben und Herausforderungen eine Schlüsselfunktion zu, denn nur durch einen methodisch sauberen und ganzheitlichen Ansatz behalten Sie den Überblick und kriegen Sie Ihre Risiken fest und nachhaltig in den Griff. Profitieren Sie darüber hinaus von Mehrwerten und Quick-Wins bei der Einführung einer gut durchdachten IT Risk Management Methodik, mit der Sie kluge Entscheidung für gezielte und effiziente Investitionen treffen können.

2. IT Risk Management, der bewusste Umgang mit Risiken

Risiken im Informationsmanagement treten auf unterschiedlichen Ebenen in zahlreichen Varianten auf. Ob als strategische oder operative IT-Risiken, ob in Form von Sicherheitslücken in der IT Infrastruktur oder in Form von Fehlfunktionen bei der Gewinnung, Weitergabe und Verwendung von Informationen. All diese IT-Risiken müssen einem Risikomanagementprozess unterworfen und somit identifiziert, analysiert, gesteuert und überwacht werden. ▶

Etwa 24 % aller mittelständischen Unternehmen in Deutschland haben ein Risikomanagement System eingeführt aufgrund bestehender Gesetze oder anderer Formalismen.*

Copyright © ICB GmbH

ICB Internet Consulting
for Business GmbH
Am Söldnermoos 17
D-85399 Hallbergmoos

Phone +49 89 1250908-0
Fax +49 89 1250908-11
Email info@icb-gmbh.de
Web www.icb-gmbh.de

Bankverbindung
Freisinger Bank
Kto-Nr. 420 78 74
BLZ 701 696 14

Handelsregister
HRB 143316 AG München
Ust-IdNr DE 223985413
Finanzamt Freising

Geschäftsführer/
Managing Director
Dipl.-Ing. Manuel Baum

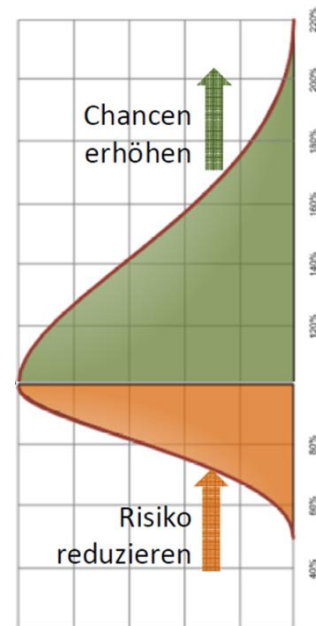
Unternehmer schätzen IT-Ausfallrisiken neben Risiken aus dem Wettbewerbs- und Marktumfeld als sehr bedrohlich ein.*

Gesetzliche Bestimmung wie beispielsweise aus dem KonTraG „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“ (§ 91 Abs. 2 AktG) aber auch zahlreiche andere gesetzliche Bestimmungen wie z.B. die Mindestanforderungen an das Risikomanagement (MaRisk) wie sie in BASEL II gefordert sind, zwingen die Unternehmen unmittelbar zur Etablierung eines funktionstüchtigen Risikomanagements.

Auch vor mittelständischen Unternehmen machen diese Bestimmungen, durch die Ausstrahlungswirkung dieser Gesetze auf andere Rechtsformen, nicht Halt. Die Gesetze geben auch hier Anlass zu einem erhöhten Risikobewusstsein, denn die Umsetzung von Maßnahmen in AGs und GmbHs werden Mindeststandards schaffen, die auch in mittelständischen Unternehmen von Geschäftspartnern und Kreditinstituten kritisch hinterfragt oder gefordert und geprüft werden.

Die Problematik in der Umsetzung der gesetzlichen Anforderungen besteht darin, dass diese meist nur schwammig formuliert sind. In der Praxis wird die Einhaltung der gesetzlichen Anforderungen oder zumindest die Erfüllung der Sorgfaltspflichten durch Compliance mit etablierten Standards, ISO-Normen oder Best Practises bspw. das Grundschutzhandbuch des Bundesamtes für Sicherheit in der Informationstechnik (GSHB der BSI), COBIT, ISO 27001, etc. nachgewiesen.

Außer zur Einhaltung von gesetzlichen sowie branchen- oder marktspezifischen Bestimmungen liegt bei der Betrachtung von IT-Risiken der Fokus häufig auf den klassischen IT-Sicherheitsaspekten. Neben Datensicherheit und Datenschutz fällt darunter insbesondere der Schutz eines IT-Systems gegen die drei Grundbedrohungen der Informationssicherheit: Verlust der Verfügbarkeit, der Vertraulichkeit und der Integrität. Es gibt es aber auch noch eine andere Betrachtungsweise, die das IT Risk Management besonders interessant erscheinen lassen:



Ein Unternehmen ist durch seine Betätigung am Markt vielfältigen Risiken ausgesetzt. Das Erwirtschaften dauerhafter risikoloser Gewinne ist praktisch unmöglich. Risiken sind Bestandteil der Geschäftstätigkeit eines jeden Unternehmers, und sich damit auseinander zu setzen gehört daher zu seinen wichtigsten Pflichten. Da Risiken also nicht vermieden werden können, sondern die wirtschaftliche Lage eines Unternehmens vielmehr von Risiken bestimmt ist, orientiert man sich stattdessen an der Wahrscheinlichkeit des Eintretens bestimmter Bedrohungen und den damit verbundenen möglichen wirtschaftlichen Schäden. Das IT-Risikomanagement beinhaltet den bewussten Umgang mit Risiken durch Erkennen der Bedrohungen, Bewerten der Risiken und die Einführung planmäßiger Sicherheitsvorkehrungen sowie deren Überwachung und Weiterentwicklung.

Entscheidungen und Maßnahmen gegen Risiken werden oft aus dem Bauch heraus getroffen. IT Risk Management führt zu quantitativ fassbaren Entscheidungsgrundlagen.

Ziel eines jeden Unternehmens muss die Optimierung seines Risiko- und Chancenprofils sein. Ein funktionierendes und effizientes Risiko-Management sowie eine gelebte Risiko- und Kontrollkultur ist als Erfolgsfaktor für Unternehmen nicht wegzudenken. Nur jene Unternehmen, die ihre Risiken effizient steuern und kontrollieren sowie ihre Chancen erkennen und nutzen, werden langfristig erfolgreich sein und den Unternehmenswert steigern können. Risiko-Management sollte daher integraler Bestandteil einer wertorientierten Unternehmenssteuerung sein und ein ausgereiftes IT Risk Management System bildet dazu eine wesentliche Grundlage, ohne die die Komplexität nicht zu beherrschen ist.

Aus dem Ernst & Young Best Practise Survey „Risikomanagement 2005“ geht hervor, dass 2/3 der nicht börsennotierten Unternehmen ihre Risiken lediglich qualitativ erfassen und nur jedes dritte Unternehmen die Wechselwirkungen zwischen den Einzelkriterien mit einbeziehen. Des Weiteren wurde festgestellt, dass in den meisten Unternehmen die Chancen als Kehrseite der Medaille „Risiko“ nicht in den Risikomanagementprozess mit einbezogen werden.

Fazit ist, dass ausgelöst durch die reine Erfüllung gesetzlicher Anforderungen in der Ausgestaltung der Risikomanagementsysteme noch Nachhol- und Optimierungsbedarf besteht, gleichzeitig aber der Trend besteht, Risikomanagement konsequent zu einem effektiven und effizienten Instrument zur systematischen Früherkennung künftiger Chancen und Risiken weiter zu entwickeln. ►

3. Erfassen und bewerten Sie die versteckten Risiken in Ihrer IT und investieren Sie in zielführende Maßnahmen



Die Zielsetzung und die Anforderungen die das Unternehmensmanagement und die IT-Verantwortlichen an das IT Risk Management und deren unterstützende Systeme haben sind genauso vielfältig wie komplex. Übergeordnete Fragestellungen wie:

- Wie viel IT braucht mein Unternehmen wirklich?
- Ist die IT im Unternehmen sicher genug?
- Ist mein Unternehmen bezogen auf IT-Sicherheit unter- oder überinvestiert?
- Sind alle relevanten Risiken zueinander ausgewogen?

IT Risk Management bezieht sich auf den bewussten Umgang mit Chancen und Risiken im Bereich der Informationstechnologie.

wollen durch das IT Risk Management genauso beantwortet werden, wie eine pragmatische Lösung für die TOP Herausforderungen die in diesem Zusammenhang an die IT-Verantwortlichen gestellt werden:

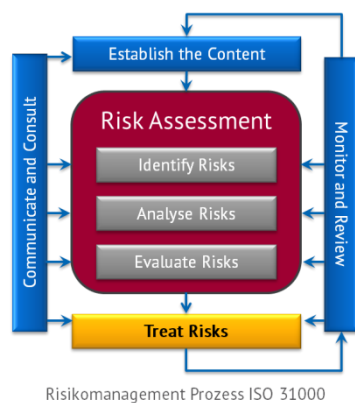
- Die Komplexität der IT managen.
- In richtige und notwendige Maßnahmen investieren.
- Den Nutzwert (ROI) von (IT-) Maßnahmen darstellen.
- Ausreichende Betriebssicherheit und Zuverlässigkeit sicherstellen.
- Notfallvorsorgen, Notfallhandbücher und Notfallplanung bereitstellen.
- Compliance zu geltende Normen, Gesetzen und Vorschriften herstellen.
- Service-Qualität und Service-Level managen.
- Den IT-Risikomanagement Prozess betreiben und kontinuierlich verbessern.

gefunden werden will. Als Antwort auf diese Fragen und Aufgabenstellungen liefert Ihnen die ICB eine Methodik und ein IT Risk-Management System, das speziell für diesen Einsatzbereich konzipiert ist und sich bewährt hat. ▶

Als Vorgehensmodell zur Einführung von IT Risk Management hat sich der Risikomanagement Prozess nach ISO 31000 etabliert, an dem sich auch die ICB orientiert. In den fünf aufeinander aufbauenden Leistungsstufen

- Content Establishment
- Scope Analysis
- Risk Assessment
- Risk Control und
- Implementation

wird der gesamte Einführungszyklus abgedeckt, der dann im Weiteren fortlaufend überwacht und kontinuierlich verbessert werden muss, um daraus nachhaltig profitieren zu können und die gesteckten Ziele zu erreichen.



Die wirklichen Mehrwerte erreicht man aber erst durch ein ausgeklügeltes IT Risk Management System, das es einem nicht nur erlaubt, die Risiken zu identifizieren und Maßnahmen zu steuern, sondern darüber hinaus:

Mit einer Cost-Benefit Analyse lassen sich IT-Risiken monetär quantifizieren und somit die Kosten-Nutzen Relation von Maßnahmen ermitteln.

- ein komplettes Abbild der IT-Infrastruktur mitsamt seiner Prozesse in seiner gesamten Ursache-Wirkung-Kette zu erfassen
- daraus auf einfachste Weise (quasi auf Knopfdruck) verschiedene Compliance Reports, wie BSI Grundschutzhandbuch, ISO 27001, ISO 20000, CoBIT, SOX u.a. zu generieren
- Simulationen über Auswirkungen von Änderungen in der IT-Architektur, den Prozessen oder Service Levels auf die Geschäftsprozesse und die Risikobewertung der IT des Unternehmens im Vorfeld von Entscheidungen durchführen zu können
- Entscheidungsgrundlagen für taktische und strategische Entscheidungen mit deren Auswirkung auf die Chancen/Risiko-Balance zu erstellen
- Eine GAP-Analyse, mit der sich die Abweichungen des Ist- zum Sollzustand darstellen lässt (sowohl negative -> unterinvestiert, als auch positive -> überinvestiert)
- eine Cost-Benefit Analyse für möglichen Maßnahmen durchzuführen, als Planungsgrundlage für gezielte Maßnahmen

- Priorisierung der Maßnahmen anhand der Gap-Analyse und dem Nutzwert, der sich daraus ergibt
- und schließlich eine quantitative Bewertung der Risiken nach einem etablierten und leicht verständlichen Bewertungssystem und als tatsächlichen wirtschaftlichen Gegenwert, der durch potenzielle Schäden und deren Eintrittswahrscheinlichkeit anhand der Abbildung der IT-Infrastruktur präzise errechnet werden kann.

Zur Erfüllung dieses Bündels an Anforderungen setzt die ICB auf die CRISAM[®] Methodologie, mit der sich all diese Anforderungen an ein IT Risk Management System erfüllen lassen.

Als Stärke dieses IT-Risk Management Systems ist hervorzuheben, dass sich, nachdem einmal eine elektronische Strukturanalyse erstellt ist, aus dem System heraus sehr einfach zahlreiche Reports erstellen, die sowohl als Planungsgrundlage, als auch zur Vorbereitung für anstehende Zertifizierungen oder als Dokumentation für Wirtschaftsprüfer dienen. Sie sind jederzeit aussagefähig über Ihre Chancen und Risiken Ihrer IT und können neue Szenarien einfach simulieren, bevor Sie eine Entscheidung fällen. Sie erkennen sofort, an welchen Stellen sie über- und unterinvestiert sind. Das Einzigartige dieses Systems ist aber, dass Sie über Ihre Risiken ein Bewertungssystem erhalten wie Sie es aus der Finanzwelt kennen (S&P) und die Risiken quantifiziert dargestellt werden. Daraus können entweder Investitionsentscheidungen gezielt getroffen werden, oder Sie akzeptieren Risiken und bilden dafür Rückstellungen, die durch die Art und Weise der Erhebung und Dokumentation auch den kritischen Prüfungen eines Wirtschaftsprüfers standhalten.

4. **ICB - Ihr verlässlicher Partner zur Einführung und Optimierung von IT Risk Management. Erhöhen Sie nachhaltig Ihre Chancen und managen Sie Ihre Risiken.**

Die ICB unterstützt Sie bei der gesamtheitlichen Bewertung Ihrer IT Architektur, Organisation und Prozesse im Rahmen einer übergreifenden IT Risk Management Analyse.

Mit unserer Erfahrung und unseren hochkarätigen Experten in den Bereichen IT Infrastrukturplanung und IT Security sowie Projektmanagement und IT-Service Management sehen wir uns als idealer Partner für Unternehmen, bei denen die IT einen bedeutenden Anteil an der Wertschöpfung des Unternehmens hat. Aus der Praxis für die Praxis ist unser Motto, nach dem wir auch das IT Risk Management in unser Leistungsportfolio aufgenommen haben, weil wir verstehen, wo wir hinschauen müssen und wissen, wie daraus Mehrwerte generiert werden können. ▶

Die vorgestellte Methodologie bietet ausgefeilte Instrumente, die durch den gesamten Prozess führen und die richtigen Fragen stellt. Mit unserer Erfahrung und dem Fingerspitzengefühl an dieser Stelle unterstützen wir Sie an der Stelle und richten Ihnen die Strukturanalyse und den Aufbau des Strukturbaumes individuell auf Ihr Unternehmen aus, führen Interviews mit den Fachbereichen, erstellen für Sie Entscheidungsvorlagen und Managementpräsentation und begleiten Sie darin, die Implementierungsprojekte richtig aufzusetzen und zu steuern. ◀