Xpert.press

Die Reihe **Xpert.press** vermittelt Professionals in den Bereichen Softwareentwicklung, Internettechnologie und IT-Management aktuell und kompetent relevantes Fachwissen über Technologien und Produkte zur Entwicklung und Anwendung moderner Informationstechnologien.

Karlheinz H. W. Thies

Management operationaler IT- und Prozess-Risiken

Methoden für eine Risikobewältigungsstrategie

Springer

Karlheinz H. W. Thies
Neckarstr. 10
61206 Wöllstadt
Karlheinz.Thies@Thies-Online.org

ISBN 978-3-540-69006-1 e-ISBN 978-3-540-69007-8

DOI 10.1007/978-3-540-69007-8

ISSN 1439-5428

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

© 2008 Springer-Verlag Berlin Heidelberg

Dieses Werk ist urheberrechtlich geschützt. Die dadurch begründeten Rechte, insbesondere die der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Eine Vervielfältigung dieses Werkes oder von Teilen dieses Werkes ist auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes der Bundesrepublik Deutschland vom 9. September 1965 in der jeweils geltenden Fassung zulässig. Sie ist grundsätzlich vergütungspflichtig. Zuwiderhandlungen unterliegen den Strafbestimmungen des Urheberrechtsgesetzes.

Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Der Verfasser hat Texte und Abbildungen mit größter Sorgfalt erarbeitet. Dennoch können Fehler nicht ausgeschlossen werden oder es können sich Anforderungen oder Rahmenbedingungen zwischenzeitlich geändert haben. Aus diesem Grund werden keine juristische Verantwortung und keine Garantie für Informationen und Abbildungen in Bezug auf Qualität, Durchführbarkeit oder Verwendbarkeit für einen bestimmten Zweck übernommen. In keinem Fall ist der Verfasser für direkte, indirekte oder Folgeschäden jedweder Art haftbar, die aus der Anwendung oder Umsetzung dieses Buches resultieren.

Einbandgestaltung: KünkelLopka, Heidelberg

Gedruckt auf säurefreiem Papier

9 8 7 6 5 4 3 2 1

springer.de

Vorwort

Grabe den Brunnen, bevor Du Durst hast
(Chinesisches Sprichwort)

Während in der heutigen Zeit die Öffnung alter Strukturen und damit auch die zugrunde liegende Technik für uns neue Chancen und Flexibilität bieten, können wir nicht außer Acht lassen, dass diese auch neue Risiken mit sich bringen.

Die Notwendigkeit, Sicherheit und Risikomanagement als permanente Prozesse im Unternehmen zu betreiben, resultiert aus verschiedenen Beweggründen. Zum einen ist es erforderlich, gegenüber Kunden und Geschäftspartnern Produkte und Dienstleistungen zuverlässig und in hoher Qualität zur Verfügung zu stellen. Zum anderen gilt es, den Fortbestand des Unternehmens zu sichern.

Die Geschäftstätigkeiten und die Geschäftsprozesse werden oftmals nur noch mit Hilfe von Informationstechnik (IT) durchgeführt. Viele Geschäftsprozesse werden elektronisch unterstützt, große Mengen von Informationen elektronisch gespeichert, genutzt, verarbeitet und teilweise in öffentlichen Netzen übermittelt. Darüber hinaus sind auch Sicherheitsaspekte wie Haus- und Gebäudeschutz, personelle Sicherheitsmaßnahmen, Arbeitsplatzschutz und im Gesamtkontext auch die Ausfall- und Kontinuitätsplanung mit zu betrachten.

Insbesondere sind die Geschäftstätigkeiten des Unternehmens in hohem Maße abhängig vom einwandfreien Funktionieren der eingesetzten IT. Dieses kann nur durch ordnungsgemäßen und entsprechend verfügbaren Einsatz der IT-Systeme und den verantwortungsbewussten Umgang aller Mitarbeiter mit den IT-Anwendungen und zugehörigen sensitiven Daten oder anderen eingesetzten Ressourcen (externe Dienstleistungen) garantiert werden. Darüber hinaus ist die Entwicklung und Erhaltung sicherer Geschäftsprozesse von entscheidender Bedeutung.

Weiterhin greifen gesetzliche Bestimmungen, Aufsichtspflichten und Verordnungen in die Geschäftstätigkeit regelnd ein. Ein großer Teil dieser Daten unterliegt dem Geschäftsgeheimnis und dem Datenschutzgesetz. Darüber hinaus gelten weitere Gesetzestexte für Finanzinstitute, wie das KWG und das WpHG. Seit 1998 sieht der Gesetzgeber mit dem KonTraG eine persönliche Haftung von Geschäftsführern und Vorständen in den Fällen vor, in denen gravierende Notsituationen oder Ereignisse frühzeitig hätten erkannt werden müssen. Diese Verpflichtung gilt auch für die Sicherheit und die Kontinuität von Geschäftsprozessen.

Sicherheitsanspruch und Risikomanagement stehen vordergründig oftmals im Interessenkonflikt mit der betriebswirtschaftlichen Seite und der Nutzen ist häufig nicht unmittelbar erkennbar. Der Anspruch bzgl. der Qualität von Produkten und Dienstleistungen für Kunden und Geschäftspartner sowie die Aufrechterhaltung der Geschäftsprozesse des Unternehmens und die Einhaltung gesetzlicher Regelungen verpflichten generell, eine sichere und funktionsfähige IT als wirtschaftliches Gut zu betrachten und als ein Unternehmensziel zu definieren.

Sicherheit und Risikomanagement können nicht alleine von der Geschäftsführung und vom Management getragen werden, sondern erfordern die Mitwirkung aller Mitarbeiter in ihrer täglichen Arbeit, um das erforderliche Niveau aufrechtzuerhalten. Die aufgeführten Verfahren und Methoden sollen zur Verbesserung und Aufrechterhaltung eines angemessenen Sicherheitsniveaus als Leitlinie im Sinne der „Best Practices“ dienen.

Inhalt

Kapitel 1
Einführung

Dieses Buch beschäftigt sich mit dem Aufbau einer IT-Sicherheitspolicy sowie mit den operationalen Risiken von Geschäftsprozessen, IT-Anwendungen und Infrastruktur, wobei hier Finanzdienstleister aufgrund der Basel-II-Anforderungen besonders im Blickpunkt stehen. Generell ist festzuhalten, dass aufgrund der Schnelllebigkeit von Produkten, Technik und organisatorischen und gesellschaftlichen Veränderungen das Ziel praktikabler und wirtschaftlicher Ansätze nach dem Pareto-Prinzip (20:80) im Vordergrund steht.

Zuerst wird die Struktur einer IT-Sicherheitspolicy dargestellt. Danach wird modellhaft gezeigt, wie operationelle Risiken ermittelt und erarbeitet werden. Vertiefend wird auf Hilfsmittel und Vorgehensweisen zur Steuerung der operationellen Risiken eingegangen. Diese Steuerung umfasst neben der Präventiv- und Notfallplanung auch das Kontinuitätsmanagement (Continuity Management). Dadurch, dass ein Großteil der hier betrachteten Faktoren so genannte weiche Faktoren sind – diese sind nur bedingt zählbar und es bedarf in vielen Fällen einer fachkundigen Einschätzung von Wahrscheinlichkeiten, Schadensverläufen sowie festzulegender Maßnahmen zur Risikobewältigung – können die folgenden Darstellungen nur als Grundgerüst für ein Risikomanagement gesehen werden.

Bei der Anwendung der hier vorgestellten Modelle und Vorgehensweisen ist eine Erweiterung und Anpassung an branchenspezifische Anforderungen erforderlich. Zur Erreichung von Revisionssicherheit und zur Minimierung von Haftungsrisiken und Gewährleistungen ist eine Abstimmung mit Revision, Wirtschaftsprüfern und Juristen unbedingt angeraten.

K. H. W. Thies, *Management operationaler IT- und Prozess-Risiken,*

© Springer 2008

Kapitel 2
IT-Sicherheitspolicy

2.1 Einordnung der IT-Sicherheitspolicy

Regelungen zur Sicherheit werden in einem Unternehmen auf drei Ebenen definiert, die im Folgenden beschrieben werden:

- **Sicherheitsgrundsätze**: Auf der obersten Ebene der Sicherheitsarchitektur befinden sich die Sicherheitsgrundsätze, die den Rahmen zur Umsetzung der Sicherheitspolitik aufzeigen und die prinzipiellen Verantwortlichkeiten festlegen.
- **Umsetzungsstrategie**: Die Umsetzungsstrategie beinhaltet weiterreichende Regeln und Strategien zu grundsätzlichen Sicherheitsanforderungen. Diese beschreiben das, was an Sicherheitsstrategien zu berücksichtigen und umzusetzen ist.
- **Sicherheitsmaßnahmen**: In den Sicherheitsmaßnahmen werden detaillierte Konzepte und als Unterbau weiterführende Anweisungen und technische bzw. organisatorische Maßnahmen festgelegt, die sich auf die aktuelle System-Plattform, auf Anwendungen oder aktuelle organisatorische Strukturen des Unternehmens beziehen. Diese Dokumente beschreiben das wie der Umsetzung der Sicherheitsstrategien.

2.2 Definition des Geltungsbereichs

Die Sicherheitsgrundsätze sind für alle Organisationseinheiten in einem Unternehmen verbindlich. Insbesondere richten sie sich an alle Mitarbeiter und externen Dienstleister, die IT-Komponenten für das Unternehmen entwickeln, betreiben oder deren Dienste vom Unternehmen selbst genutzt werden. Falls eine netzwerktechnische Anbindung für einen Dritten (Kunde) nicht entsprechend dem Sicherheitsstandard gestaltet werden kann, sind die Sicherheitsgrundsätze und die daraus abgeleiteten Regelungen auch für diesen bindend.

© Springer 2008

Die Sicherheitspolitik wird in Abstimmung mit der Geschäftsführung erstellt und von dieser verabschiedet. Die aktuelle Version wird zeitnah veröffentlicht und kommuniziert.

Ausnahmen, die von den Sicherheitsgrundsätzen und den untergelagerten Umsetzungsstrategien und Sicherheitsmaßnahmen abweichen oder diese nicht berücksichtigen, sind durch eine Entscheidungs-Vorlage mit der Begründung der Nichteinhaltung und den daraus entstehenden Risiken zu dokumentieren und müssen per Beschluss von der Geschäftsführung genehmigt werden.

2.3 Sicherheitsgrundsätze

Die Sicherheitsgrundsätze definieren die Sicherheitspolitik eines Unternehmens.

2.3.1 Sicherheitsgrundsatz 1: Unternehmensziel

Eine sichere Informationsverarbeitung ist unabdingbare Voraussetzung für alle Geschäftsprozesse im Unternehmen. Die Geschäftsleitung sieht die Sicherheit daher als integralen Bestandteil der Unternehmenspolitik an.

Aufgrund der Abhängigkeit der Geschäftsprozesse von der Informationsverarbeitung müssen Sicherheitsaspekte bei der Gestaltung und Umsetzung dieser Geschäftsprozesse besonders berücksichtigt werden. Die Ziele des Unternehmens können nur bei ordnungsgemäßer und verlässlicher Abwicklung der Geschäftsprozesse erreicht werden.

Ein hohes und unter betriebswirtschaftlichen Gesichtspunkten vertretbares Sicherheitsniveau dient dem Schutz des gesamten Unternehmens, der Geschäftspartner, Kunden und Mitarbeiter. Aus diesem Grund werden umfangreiche, fortlaufende Sicherheitsmaßnahmen in allen Bereichen ergriffen, um berechtigte Interessen der Geschäftspartner, Kunden und Mitarbeiter zu schützen.

2.3.2 Sicherheitsgrundsatz 2: Schadensvermeidung

Ein Sicherheitsziel ist es, operationale Risiken durch Vorsorgemaßnahmen zu mindern und Schäden frühstmöglich entgegenzuwirken.

Risiken im Ablauf der Geschäftsprozesse und der genutzten Informationsverarbeitung zählen zu den operationalen Risiken im Unternehmen. Diese Risiken sind unter Berücksichtigung wirtschaftlicher Aspekte auf ein vertretbares Maß zu reduzieren.

Der Aufwand für die Schadensvermeidung hängt im Wesentlichen davon ab, welche Risiken im Bereich der Sicherheit vertretbar sind. Für die untragbaren Risiken sind geeignete Maßnahmen zu finden, um diese auf ein vertretbares Maß zurückzustufen. Die Maßnahmen können dabei die Reduktion der Eintrittswahrscheinlichkeit und/oder die Schadenshöhe beeinflussen. Die Kosten dieser Maßnahmen müssen in einem angemessenen Verhältnis zum vermiedenen Schaden stehen.

2.3.3 Sicherheitsgrundsatz 3: Sicherheitsbewusstsein

Alle Mitarbeiter müssen über ein ausgeprägtes Sicherheits- und Qualitätsbewusstsein bei der von ihnen ausgeübten Arbeit verfügen. Dieses verpflichtet einerseits jeden Mitarbeiter, bestehende Sicherheitsregelungen zur Kenntnis zu nehmen und anzuwenden, und andererseits, unverzüglich zuständige Führungskräfte oder Security-Beauftragte[1] über vorliegende Sicherheitsrisiken zu informieren.

Ein ausgeprägtes Sicherheits- und Qualitätsbewusstsein der Mitarbeiter ist Voraussetzung für eine erfolgreiche Planung, Umsetzung und Aufrechterhaltung der Sicherheit innerhalb des Unternehmens. Die Früherkennung möglicher Sicherheitsrisiken und deren sofortige Beseitigung sind im Interesse des Unternehmens sowie seiner Geschäftspartner von allen Mitarbeitern im Rahmen der täglichen Arbeit zu leisten. Insgesamt müssen Risiken konsequent auf ein akzeptables Risikoniveau gesenkt werden. Die Mitarbeiter müssen daher entsprechend sensibilisiert sein und durch geeignete Schulungen und/oder Informationen auf dem neuesten Stand gehalten werden. Hierbei ist die Verfügbarkeit und Aktualität der zugehörigen Dokumentationen von besonderer Bedeutung.

2.3.4 Sicherheitsgrundsatz 4: Gesetzliche, aufsichtsrechtliche und vertragliche Pflichten

Gesetzliche und aufsichtsrechtliche Verpflichtungen sowie vertragliche und unternehmensinterne Vorgaben an die Informationsverarbeitung sind zu erfüllen und dienen dem Schutz der Kunden, Geschäftspartner, Mitarbeiter und Anteilseigner des Unternehmens sowie des Unternehmens selbst.

Sicherheitsanforderungen und Sicherheitsmaßnahmen werden auf der Grundlage sicherheitsrelevanter gesetzlicher, aufsichtsrechtlicher und vertraglicher Re-

[1] Ansprechpartner, Koordinator zu Sicherheits-Themen im Fachbereich.

gelungen festgelegt. Änderungen oder neue Regelungen erfordern entsprechende Aktualisierung der Sicherheitskonzepte, Anweisungen und Maßnahmen sowie deren zeitnahe Umsetzung.

2.3.5 Sicherheitsgrundsatz 5: Maßnahmen gemäß allgemeingültiger Sicherheitsstandards

Daten und Ressourcen des Unternehmens sind in hohem Maße durch technische und organisatorische Maßnahmen gemäß allgemeingültiger Sicherheitsstandards und -richtlinien zu schützen. Diese Maßnahmen dienen der Erreichung des gesetzten IT-Sicherheitsstandards. Zur grundsätzlichen Orientierung dienen das BSI-Grundschutzhandbuch sowie die einschlägigen Normen.

Die erforderlichen Sicherheitsmaßnahmen werden für alle Daten und Ressourcen geplant und umgesetzt sowie bei Veränderungen der Sicherheitsanforderungen kontinuierlich angepasst. Insbesondere müssen die Maßnahmen in ihrer Umsetzung sicherstellen, dass ein angemessener Schutz der Verfügbarkeit, der Vertraulichkeit, der Integrität, der Verbindlichkeit und Authentizität der Daten und Ressourcen erreicht wird und der störungsfreie und korrekte Ablauf aller Geschäftsprozesse gewährleistet ist. Soweit betriebswirtschaftlich vertretbar, sind die redundante Auslegung geschäftskritischer Anwendungen und Systeme, Backup und Bereitstellung aktueller Notfallkonzepte für die Kerngeschäftsprozesse des Unternehmens von sehr hoher Bedeutung.

2.3.6 Sicherheitsgrundsatz 6: Aufrechterhaltung des Geschäftsbetriebes

Das mögliche Schadenspotenzial bei Störungen der Kerngeschäftsprozesse ist steuerbar. Geschäfte können auch in Krisen- und Notfallsituationen in vertretbarem Maß getätigt und abgewickelt werden.

Für geschäftskritische IT-Systeme und IT-Anwendungen existieren Notfall- und Kontinuitätspläne, die unter Berücksichtigung bestehender Verfügbarkeitsanforderungen Vorgehensweisen spezifizieren für:

- den eingeschränkten Betrieb oder die kontrollierte Einstellung des Betriebs;
- den geregelten Wiederanlauf.

Zuständig für Aktualisierung und Durchführung der in den Notfallplänen festgelegten Aktivitäten ist der jeweilige verantwortliche Eigentümer des Geschäftsprozesses. Ebenfalls ist sicherzustellen, dass Mitarbeiter und auch Dienstleister, die IT-Anwendungen, Komponenten und Systeme betreiben und betreuen, mit den entsprechenden Vorgehensweisen vertraut sind und diese im Rahmen regelmäßiger Übungen praktizieren.

2.3.7 Sicherheitsgrundsatz 7: Sicherheitsarchitektur

Die Umsetzung der Sicherheitspolitik erfolgt durch eine verbindliche Sicherheitsarchitektur, die von dem Sicherheits-Team des Unternehmens vorgegeben und kontinuierlich weiterentwickelt wird.

Die Sicherheitsarchitektur integriert sicherheitsrelevante Elemente wie Sicherheitsgrundsätze, -anforderungen, -maßnahmen und -dienste und ermöglicht eine zielgerichtete Umsetzung der Sicherheitspolitik innerhalb des Unternehmens. In der Sicherheitsorganisation werden Verantwortlichkeiten sowie ausreichende Kompetenzen zur Behandlung sicherheitsrelevanter Vorkommnisse vergeben. Die Umsetzung der festgelegten Sicherheitsziele erfolgt durch organisatorische und technische Maßnahmen.

2.4 Verantwortlichkeiten

2.4.1 Geschäftsführung und Management

Die Gesamtverantwortung für die Sicherheit innerhalb des Unternehmens liegt bei der Geschäftsführung. Sie ist insbesondere verantwortlich für:

- die Überprüfung, die Abnahme und das Vertreten der Sicherheitspolitik und
- die Weiterentwicklung der Sicherheitsorganisation.

In beratender, empfehlender und unterstützender Form nimmt diese Aufgabe das Sicherheits-Team (IT-Security-Officer) für die Geschäftsführung wahr.

Zur Erreichung eines angemessenen Sicherheitsniveaus tragen die Mitarbeiter im Management eine besondere Verantwortung. Sie müssen sicherstellen, dass im Rahmen der Umsetzung der ihnen und ihren Mitarbeitern übertragenen Aufgaben die Sicherheitsaspekte entsprechend berücksichtigt werden. Dazu gehört insbesondere die Sensibilisierung der Mitarbeiter sowie die Implementierung und Kontrolle von Sicherheitsmaßnahmen.

2.4.2 Sicherheitsorganisation

Die Umsetzung der Sicherheitsgrundsätze erfolgt durch die Sicherheitsorganisation sowie durch alle Mitarbeiter entsprechend ihren Aufgaben in der Linie. Den IT- und fachlichen Administratoren fällt eine besondere Rolle zu, da der sichere Betrieb von IT-Systemen und IT-Anwendungen eine der tragenden Säulen der Umsetzung darstellt.

Die Prüfung der Umsetzung und Einhaltung der Sicherheitsgrundsätze obliegt dem Sicherheits-Team gemeinsam mit den zuständigen Security-Beauftragten; situativ werden das Controlling (Risk-Controlling) und die Revision zusätzlich mit eingebunden. Unabhängig davon prüft die Revision im Rahmen ihrer Prüfpläne u. a. auch die Einhaltung von Sicherheitsmaßnahmen, die aus gesetzlichen und aufsichtsrechtlichen Anforderungen resultieren.

Mit der für das Controlling zuständigen Organisationseinheit erfolgt eine metho-dische und prozessuale Abstimmung bezüglich des Themas „Operationale Risiken“.

Die Sicherheitsorganisation wird gebildet aus:

- dem Sicherheits-Team (IT-Security-Officer, Team in der Abt. Organisation & Service);
- den Security-Beauftragten (mindestens ein Mitarbeiter je Bereich/Hauptabteilung);
- den Sicherheitsadministratoren (IT-Anwendungs- und IT-Systembetreuung, RZ-Betrieb);
- der Berechtigungsverwaltung.

Aufgaben des Sicherheits-Teams sind:

- Erarbeitung und Weiterführung der Sicherheitsstrategien, -regeln, -konzepte, -anweisungen und -maßnahmen;
- Allgemeine Beratung und Unterstützung zum Thema Sicherheit;
- Projektbegleitende Beratung zur Sicherheitskonzeption auf Anforderung des Fachbereichs und Prüfmaßnahmen bei der Übergabe von Projekten;
- Mitarbeitersensibilisierung und -schulung in Kooperation mit der Abteilung Personal;
- Bearbeitung und Auswertung von Sicherheitsvorfällen zur Lokalisierung von Schwachstellen;
- Prüfung der Umsetzung von Sicherheitsgrundsätzen, Umsetzungsstrategien und Sicherheitsmaßnahmen;
- Kontrolle und Überwachung der Durchführung regelmäßiger Prüfungen sicherheitskritischer Anwendungen und Systeme;
- Situative und ereignisbezogene Initiierung von Sicherheits-, Risikoüberprüfungen und Notfallübungen.

Aufgaben der Berechtigungskoordination als Funktion im Sicherheitsteam:

- Erstellung und Pflege von Berechtigungskonzepten (Rollendefinition, Neuanlage/Änderung/Löschung von Berechtigungen, Automatisierung der Pflege, Infodienste);
- Formal-, Plausibilitätsprüfung und Koordination aller Berechtigungsvergaben;
- Einholung notwendiger Zustimmungen für die Berechtigungsvergabe.

Aufgaben des Security-Beauftragten im Fachbereich:

- Erste Anlaufstelle für alle Mitarbeiter des Fachbereiches zu Sicherheitsfragen und -problemen;
- In Gefahren- oder Krisensituationen Einleitung von Sofortmaßnahmen zur Schadensvermeidung oder Schadensbegrenzung;
- Eskalation und Weitergabe von Informationen an Linienvorgesetzte und an das Sicherheits-Team;
- Bearbeitung von Sicherheitsvorfällen und Erstellung von Statusberichten;
- Mitwirkung an der Verbesserung und Aktualisierung der Sicherheitsregeln, -konzepte, -anweisungen und -maßnahmen;
- Koordination und Unterstützung bei Sicherheitsthemen (Projektbegleitung, Audits, Ausfallübungen, Schulung, Einweisung).

Aufgaben der Sicherheitsadministratoren des operationalen IT-Betriebs:

- Installation, Betrieb von IT-Sicherheitseinrichtungen;
- Überwachung von IT-Systemen und Durchführung von Kontrollmaßnahmen;
- Second-Level-Support bzgl. IT-Sicherheitseinrichtungen.

Aufgaben der jeweils zuständigen Berechtigungsverwaltung:

- Administration von Zugriffsrechten für die jeweiligen IT-Anwendungen und IT-Systeme;
- Verwaltung von technischen Accounts, wobei die Administration selbst an die zuständigen Systemadministratoren delegiert wird;
- zeitnahe Dokumentation und Fortschreibung der Berechtigungen.

Bei der Einführung neuer oder bei gravierenden Änderungen bestehender IT-Anwendungen oder IT-Systeme sind angemessene und dem Standard entsprechende Sicherheitskonzepte zu erstellen und zu implementieren. Das Sicherheitsteam berät auf Anforderung des Fachbereichs die Projekte und Aktivitäten bezüglich der Sicherheitskonzeption und überprüft bei der Übergabe im Rahmen eines Projekts die Schutzbedarfsfeststellung und das Sicherheitskonzept. Sofern sicherheitsrelevante Anwendungen oder Systeme durch Dritte betrieben werden, sind zum einen Sicherheitsanforderungen vertraglich zu regeln, zum anderen ist von diesen nachzuweisen, dass angemessene Schutzmaßnahmen implementiert sind.

Falls eine netzwerktechnische Anbindung aus betriebswirtschaftlichen oder technischen Gründen nicht entsprechend den Sicherheitsregeln, -konzepten und -anweisungen realisiert werden kann, sind die Sicherheitsgrundsätze und die daraus abgeleiteten Regelungen auch für diesen Netzwerkpartner (Dienstleister, Kunde)

bindend. Bei Gefährdungen oder Sicherheitsvorfällen, die gemeinsam genutzte Ressourcen betreffen, sind diese Netzwerkpartner in die Eskalationsverfahren und Meldewege mit einzubinden.

Zum Informations- und Erfahrungsaustausch dient ein Arbeitskreis „Sicherheitsmanagement“, an dem das Sicherheits-Team, der DSB, das Service-Management (Provider-Management), Revision, Personal, Berechtigungsverwaltung, Security-Beauftragte, Sicherheitsbeauftragte von Dienstleistern sowie weitere Gäste teilnehmen. Themenvorschläge kann jeder Beteiligte der Sicherheitsorganisation einbringen. Das Sicherheits-Team sammelt die Themen, bereitet die Agenda vor und beruft den Arbeitskreis ein.

2.4.3 Mitarbeiter

Geschäftsführung, Management und Sicherheitsorganisation können vielfach nur die Rahmenbedingungen für die sichere Nutzung, Entwicklung und den Betrieb der IT schaffen. Eine Erreichung der gesteckten Ziele ist wesentlich davon abhängig, dass jeder Mitarbeiter die vorliegenden Sicherheitsgrundsätze und die daraus abgeleiteten Umsetzungsstrategien und Sicherheitsmaßnahmen beachtet und im Rahmen der täglichen Arbeit umsetzt.

Es wird ein ausgeprägtes Sicherheitsbewusstsein von jedem Einzelnen erwartet, damit:

- notwendige Maßnahmen zur Erkennung und Abwendung von Bedrohungen für die Sicherheit von Personen, Informationen und Vermögenswerten eingeleitet werden,
- Problemsituationen schnell und zuverlässig bewältigt werden,
- Risiken identifiziert und an die Verantwortlichen berichtet werden und
- Sicherheit ein Element der Unternehmensphilosophie wird.

Aufgrund von thematischen Überschneidungen zum Gebäudemanagement, das für den Gebäudeschutz zuständig ist, sind insbesondere auch diese Sicherheits- und Verhaltenshinweise bindend.

2.5 Umsetzung

2.5.1 Sicherheitsarchitektur

Ziel der Sicherheitsarchitektur ist es festzulegen, wie die Sicherheit im Unternehmen umgesetzt wird (siehe Abb. 1). Die **Sicherheitsgrundsätze** bilden die oberste Ebene der Sicherheitsarchitektur und legen allgemeine Sicherheitsgrundsätze und Verantwortlichkeiten fest. Die Sicherheitsgrundsätze gelten für das gesamte Unternehmen.

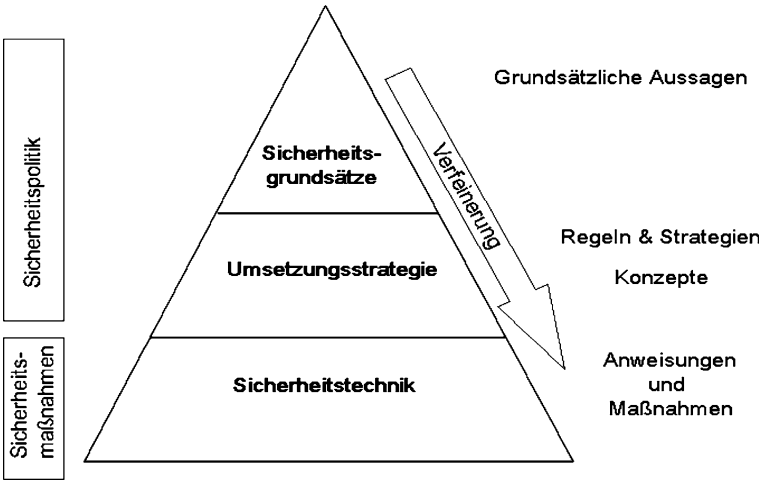


Abb. 1 Sicherheitsarchitektur

Durch die **Umsetzungsstrategie** mit ihren Regelungen werden grundsätzliche Sicherheitsanforderungen und Sicherheitsmaßnahmen beschrieben. Die Regelungen und Strategien gelten ebenfalls für das gesamte Unternehmen.

Die Umsetzungsstrategie wird durch die **Sicherheitsmaßnahmen** ergänzt; wobei in Konzepten und Anweisungen detailliert die Sicherheitsanforderungen und technische bzw. organisatorische Maßnahmen festgelegt werden, die sich auf die aktuelle System-Plattform, IT-Anwendungen oder auch auf die organisatorische Struktur des Unternehmens beziehen.

Da wegen der Kurzlebigkeit von Software und IT-Systemen häufiger mit einer Änderung und damit mit einer kürzeren Lebensdauer von Sicherheitsmaßnahmen zu rechnen ist, wird eine Trennung von Umsetzungsstrategie und Sicherheitsmaßnahmen empfohlen.

Für spezifische Sicherheitsanforderungen ist die Erstellung von zugeschnittenen Sicherheitskonzepten notwendig, weil sich die abgeleiteten Schutzmaßnahmen von Fall zu Fall unterscheiden.

Sicherheitskonzepte werden in der Regel projekt-, bzw. entwicklungsbegleitend erstellt. Stellt sich heraus, dass bei bestehenden Anwendungen oder Systemen keine ausreichende Sicherheitskonzeption vorhanden ist, so ist diese nachträglich innerhalb einer mit dem Sicherheits-Team abgestimmten Übergangsfrist zu entwickeln und zu implementieren. Bei der Erstellung von Sicherheitskonzepten ist insbesondere auf den betriebswirtschaftlichen Aufwand zur Risikominimierung zu achten und das mögliche Restrisiko darzustellen.

2.5.2 Aufgabengebiete

Sicherheit ist in nahezu allen Bereichen des Unternehmens ein Aspekt, wobei der Fokus primär auf der Informationstechnologie liegt. Speziell hier kann entsprechend nur durch kontinuierliche Bearbeitung, Verbesserung und Anpassung eine angemessene IT-Sicherheit aufrechterhalten werden.

Neben den bereits definierten Aufgabengebieten sind im Folgenden als Ausblick wichtige Themen der Sicherheit genannt, die durch die Geschäftsführung, das Management, die Sicherheitsorganisation und die jeweils verantwortlichen Mitarbeiter entsprechend der ihnen übertragenen Verantwortung bearbeitet werden müssen:

- Plattform- und Netzwerksicherheit,
- Sicherheits-Reviews und Auditing,
- IT-Risikomanagement,
- Infrastruktursicherheit,
- Zugangs- und Zugriffskontrolle,
- Sicherheitsberatung,
- Betriebssicherheit,
- Sicherheitsbewusstsein des Personals,
- Sicherheitstechnologie und -grundlagen,
- Anwendungssicherheit.

In den Umsetzungsstrategien werden die Aufgabengebiete jeweils separat und detaillierter beschrieben.

2.5.3 Kontrolle

Nach dem Grundsatz der Nachvollziehbarkeit ist der Umgang mit sicherheitsrelevanten IT-Systemen und -Anwendungen so zu gestalten, dass Verstöße gegen dokumentierte und freigegebene Sicherheitsregelungen feststellbar und ihren Verursachern zuordenbar sind. Die durchgeführten Maßnahmen dienen ausschließlich der Aufrechterhaltung der Sicherheit sowie der Einhaltung der gesetzlichen und aufsichtsrechtlichen Vorgaben und der internen Regelungen. Ein Missbrauch für andere Zwecke, insbesondere hinsichtlich der systematischen Überwachung der Mitarbeiter, ist nicht erlaubt.

Nachweisliche Verstöße gegen Sicherheitsregelungen können je nach Schwere zu Disziplinar-, arbeits- wie auch zivilrechtlichen Maßnahmen oder strafrechtlicher Verfolgung führen. Die entsprechenden Maßnahmen regelt der Bereich Personal. Bei mitbestimmungsrelevanten Themen ist der Betriebsrat mit einzubinden.

Verstöße gegen die Sicherheitsregelungen basieren unter anderem auf:

- der Nichtbeachtung sowie Verletzung gesetzlicher Vorgaben,
- dem Nichtbeachten oder Verletzen von Sicherheitsvorschriften,

- der Manipulation oder Umgehung bestehender Sicherheitseinrichtungen,
- der vorsätzlichen Schädigung des Unternehmens durch Nichterfüllung von Sicherheitsmaßnahmen,
- der Schädigung der Sicherheit von Kunden, Geschäftspartnern und Mitarbeitern durch Nichterfüllung von Sicherheitsmaßnahmen,
- der unautorisierten Preisgabe von Geschäftsgeheimnissen und vertraulichen Interna,
- der unautorisierten Veränderung sicherheitsrelevanter IT-Anwendungen, -Systeme oder anderer Vorrichtungen,
- der Nutzung von IT-Anwendungen und -Systemen für unzulässige Zwecke,
- der Verletzung der Informationspflicht beim Auftreten sicherheitsrelevanter Vorfälle.

Kapitel 3
Operationale Risiken

3.1 Grundbetrachtung der operationalen Risiken

3.1.1 Warum sind die operationalen Risiken für ein Unternehmen zu berücksichtigen?

Jedes Unternehmen entwickelt Produkte und/oder Dienstleistungen und bietet diese seinen Kunden an. Durch diese Geschäftstätigkeit alleine leitet sich schon eine Sorgfaltspflicht und Haftung gegenüber dem Kunden, aber auch gegenüber den Behörden und dem Gesetzgeber ab. Mit vermehrtem Einsatz von IT, durch Fusionierung, Outsourcing und auch durch die Globalisierung werden Geschäftsprozesse komplexer und die Anzahl möglicher Störfaktoren erhöht sich ebenfalls. Jede kleine Störung oder jedes Ereignis auf der Welt hat in vielen Fällen (wie z. B. 11. September 2001) Auswirkungen auf die eigene Geschäftstätigkeit.

Um Produkte/Dienstleistungen in der erforderlichen Art und Weise anbieten zu können, ist der reibungslose Ablauf von Geschäftsprozessen erforderlich. Für den Ablauf eines Geschäftsprozesses wiederum ist das Zusammenspiel von Informations- und Kommunikationstechnik, Mensch und Infrastruktur notwendig.

Da Störungen von Geschäftsprozessen niemals ausgeschlossen werden können, ist sicherzustellen, dass das Schadenspotenzial bei Störungen der Kerngeschäftsprozesse steuerbar ist, so dass Geschäfte in Krisensituationen auch dann noch in einem vertretbaren Rahmen getätigt werden können. Hierunter ist zu verstehen, dass bei Störungen der wichtigen Geschäftsprozesse der Geschäftsbetrieb unter betriebswirtschaftlich und unternehmerisch vertretbaren Aspekten kontrolliert und steuerbar aufrecht erhalten oder aber bewusst eingestellt wird, um das Schadenspotenzial für das Unternehmen zu optimieren.

Um dieses Ziel der Schadensoptimierung bzw. -vermeidung zu erreichen und somit eigenen Anforderungen sowie gesetzlichen Vorgaben zu genügen, ist die Einrichtung einer Funktion „IT-Security & Contingency Management“ anzuraten.

K. H. W. Thies, *Management operationaler IT- und Prozess-Risiken,*

© Springer 2008

3.1.2 Übersicht Risiken

Jedes Unternehmen ist bei der Wahrnehmung seines Geschäfts verschiedenen Risiken ausgesetzt. Risiken werden zum Teil bewusst zur Wahrung von Geschäftschancen in Kauf genommen. Risiko, d. h. die negative Abweichung von dem Erwartungswert und somit die Gefahr unerwarteter Verluste, und Rendite stehen hierbei in einem engen Zusammenhang.

Im Folgenden werden die wichtigsten Risiken (siehe auch Abb. 2) betrachtet, die für eine Gesamtrisikobetrachtung mindestens berücksichtigt werden sollten:

Marktpreisrisiko: Hierunter wird potenzieller Verlust verstanden, der unter nachhaltigen Veränderungen von Marktpreisen oder preisbeeinflussenden Parametern entstehen kann.

Ausfallrisiko: Unter Ausfallrisiko ist der potenzielle Verlust zu verstehen, der sich aus der Nichterfüllung durch den Geschäftspartner ergeben kann.

Liquiditätsrisiko: Unter Liquiditätsrisiko wird der potenzielle Verlust verstanden, der dadurch entstehen kann, dass bei Fälligkeit von Zahlungsverpflichtungen keine ausreichenden Mittel zur Erfüllung vorhanden sind.

Strategisches Risiko: Dabei handelt es sich um das Erfolgsrisiko, das primär aus Grundsatzentscheidungen zur Positionierung des Unternehmens bezüglich Kunden und Produkten, Kooperationen und Allianzen sowie zur internen Strategieumsetzung resultiert, die das Management vor dem Hintergrund gegebener Umfeldbedingungen trifft.

Operationales Risiko: Hierunter versteht man potenzielle Verluste aus Handlungen oder Maßnahmen, die aus internen Faktoren – aufbauorganisatorische, ablauforganisatorische oder technische Schwachstellen – oder auf externe Faktoren (z. B.

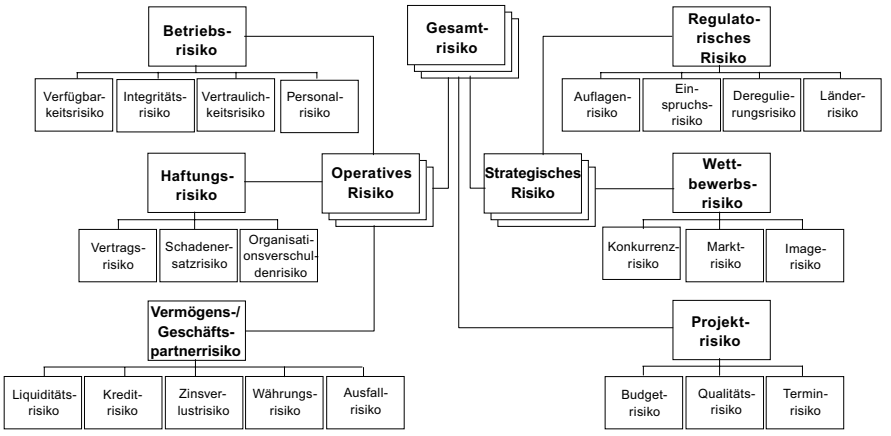


Abb. 2 Risiken nach KonTraG

Katastrophen) zurückzuführen sind. Das operationale Risiko (siehe Abb. 3) kann wie folgt weiter untergliedert werden:

Personalrisiko: Dem Personalrisiko wird die Gefahr zugeordnet, nicht in ausreichendem Maße qualifiziertes Personal zur Verfügung zu haben, sei es wegen ungewollter Unternehmensaustritte, plötzlichem Ausfall, Fehlbesetzungen oder wegen zurückgehaltener Leistungen bzw. fehlender Motivation.

Geschäftsprozessrisiko: Das Geschäftsprozessrisiko umschreibt die Gefahr mangelhafter bzw. unsicherer Geschäftsabläufe. Gründe hierfür sind nicht klar vorgegebene Verfahren, unzureichend definierte Schnittstellen, unklare Qualitätsmerkmale, gravierende Ablauf- und Medienbrüche, undefinierte Zuständigkeiten, instabile Soft- und Hardware, fehlender Datenschutz, Möglichkeiten der Manipulation, Spionage und Sabotage, mangelnde Ausfallvermeidungsmaßnahmen sowie fehlende Vorkehrungen zur Bewältigung gravierender Störungen und Unterbrechungen von Geschäftsprozessen.

Rechtsrisiko: Ein Rechtsrisiko besteht durch die Gefahren, die sich durch anhängige Prozesse, veränderte rechtliche Rahmenbedingungen und die mangelnde Durchsetzbarkeit von Verträgen (z. B. in Form von Service Level Agreements) ergeben.

Katastrophenrisiko: Das Katastrophenrisiko umschreibt Risiken, die sich aus Naturkatastrophen oder sonstigen gravierenden externen Faktoren ergeben. Hierunter zählen beispielsweise Brand, Hochwasser, Blitzschlag, Sturm, Verseuchung, Bombenanschlag und Geiselnahme. Ausschlaggebend ist bei diesen Ereignissen, dass der Geschäftsbetrieb gravierend beeinträchtigt wird und das Unternehmen in seiner Existenz gefährdet ist.

Abb. 3 Zu betrachtende operationale Risiken

Reputationsrisiko: Das Reputationsrisiko erfasst die Gefahr der Verschlechterung des Ansehens des Unternehmens durch mangelnde Kundenzufriedenheit, durch selbst- oder fremdbestimmte Imageverluste. Mögliche Konsequenzen sind Abwanderung von Kunden, aber auch von Lieferanten und Dienstleistern zu Mitbewerbern.

Technologierisiko: Das Technologierisiko erfasst die Gefahren, die sich aus der eingeschränkten Funktionsfähigkeit oder vollständigen Funktionsunfähigkeit von Hardware, Software, Haustechnik und sonstigen Technologien ergibt. Hierzu zählen auch falsch gewählte Technologie- und Prozessentscheidungen, die nicht oder nur mit an die Belastungsgrenzen des Unternehmens gehenden Aufwendungen rückgängig gemacht werden können.

Gefahren, die in den Bereichen der Hardware, DV-Infrastruktur sowie der System- und Anwendungssoftware bestehen, werden allgemein als operationale IT-Risiken zusammengefasst.

3.1.3 Gesetzliche und „quasigesetzliche" Vorgaben

Eine Vielzahl von Regelungen des Gesetzgebers und Richtlinien bzw. Verlautbarungen von Aufsichtsämtern prägt die Geschäftstätigkeit eines jeden Unternehmens. Um der Fülle dieser und auch eigener Anforderungen zu begegnen, sind der Aufbau eines Regelwerks sowie die Einrichtung eines Überwachungssystems vorzusehen. Als Teil einer Gesamtorganisation Risikomanagement ist dementsprechend auch ein „IT-Security & Contingency Management" oder zumindest ein Security-Officer zu implementieren.

3.1.4 KonTraG (u. a. Änderungen des AktG und des HGB)

Vorrangig haben sich für alle Aktiengesellschaften, die an der Börse gehandelt werden, Neuerungen durch die Einführung des KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich), mit Wirkung vom 1. Mai 1998, ergeben. Das KonTraG fasst eine Vielzahl von Einzelgesetzen zusammen (siehe Abb. 4), wie z. B. Aktiengesetz, Handelsgesetz, Genossenschaftsgesetz und Wertpapierhandelsgesetz.

Sinn und Zweck des Gesetzes sind Verbesserungen im Rahmen der Arbeit des Aufsichtsrats, Erhöhung von Transparenz, Stärkung der Kontrolle durch die Hauptversammlung, Verbesserung der Qualität der Abschlussprüfung und der Zusammenarbeit von Abschlussprüfer und Aufsichtsrat etc.

In der Fülle der gesetzlichen Änderungen, die das KonTraG bewirkt, sind, im Bezug auf das Notfall- und Krisenmanagement eines Unternehmens, nur die Änderungen des Aktiengesetzes und, mit Einschränkung, die Änderungen des Handelsgesetzbuches relevant.

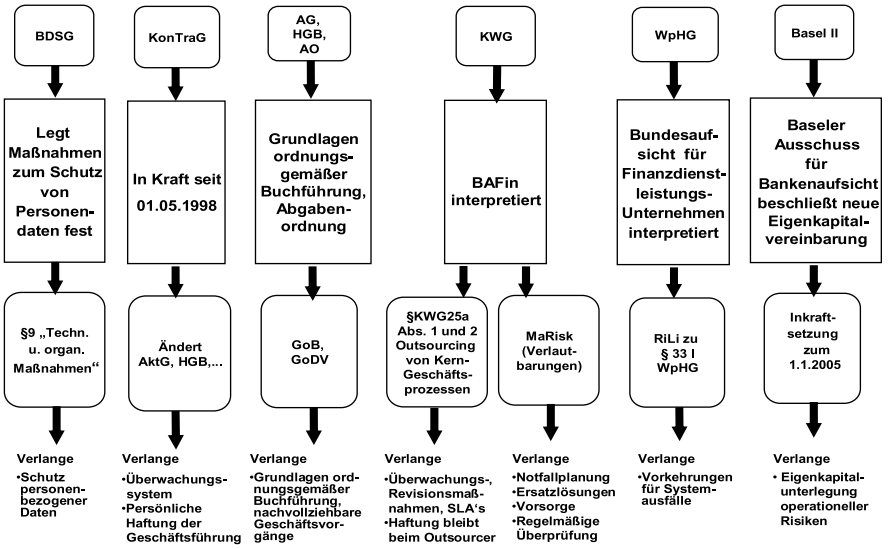


Abb. 4 Gesetzliche Rahmenbedingungen (Beispiel Finanzdienstleister)

§ 91 AktG wurde dahingehend geändert, dass ihm folgender Absatz angefügt wurde: „Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.“

Was wollte der Gesetzgeber hiermit zum Ausdruck bringen?

Der Gesetzgeber will verdeutlichen, dass dem Vorstand eine Verpflichtung obliegt, für ein angemessenes Risikomanagement und für eine angemessene interne Revision zu sorgen. Hierbei handelt es sich um eine gesetzliche Hervorhebung der allgemeinen Leitungsaufgabe des Vorstands gemäß § 76 AktG.

Die konkrete Ausgestaltung der Pflicht ist von äußeren Faktoren des Unternehmens abhängig, wie Größe, Branche, Struktur, Kapitalmarktzugang, etc. Dementsprechend ist die Organisationspflicht bei jedem Unternehmen hoch, bei einem Konzern sogar sehr hoch anzusetzen.

Das heißt: Maßnahmen interner Überwachung sollen so eingerichtet sein, dass die den Fortbestand der Gesellschaft gefährdenden Entwicklungen früh erkannt und Gegenmaßnahmen ergriffen werden können, bezogen auf bestehende (Ausfall eines Produkts) und zukünftige (Einführung eines neuen Produkts) Risiken. Risikomanagement erfordert demnach die Identifikation, Analyse, Bewertung und Steuerung von Risiken.

Bei Mutterunternehmen im Sinne des § 290 HGB ist die Überwachungs- und Organisationspflicht konzernweit zu verstehen, sofern von Tochtergesellschaften den Fortbestand der Gesellschaft gefährdende Entwicklungen ausgehen können.

Aufgrund dieser gesetzlichen Hervorhebung wird der korrespondierende § 317 IV HGB geändert und somit der Umfang der Abschlussprüfung erweitert. Der Abschlussprüfer hat nunmehr zu beurteilen, ob der Vorstand ein Überwachungssystem

eingerichtet hat und ob dieses Überwachungssystem eine Aufgabe erfüllt (vgl. in dem Zusammenhang auch §§ 321 IV, 322 I, IV HGB).

Durch die Einführung des KonTraG, insbesondere des § 91 II AktG, ergeben sich keine „wesentlichen“ Änderungen bezogen auf die Einrichtung eines Risikocontrollings in einem Unternehmen. Die Verpflichtung des Vorstands zur Einrichtung eines Überwachungssystems wird in § 91 II AktG nunmehr klarstellend erwähnt. Die explizite gesetzgeberische Hervorhebung eines Überwachungssystems lässt den Schluss zu, dass weitere und höhere Anforderungen an Organisationspflichten gestellt werden (siehe Abb. 4).

Kapitel 4
Aufbau eines Managements operationaler IT-Risiken

4.1 IT-Risikobetrachtung über ein Schichtenmodell

Die Risikobetrachtung baut auf ein Dreischichtenmodell auf (siehe Abb. 5).

- *Schicht 1* umschreibt einerseits den Haus- und Gebäudeschutz, andererseits auch mögliche K-Fall-Szenarien. Zum Gebäudeschutz gehören Zugangsberechtigung, Außenhautüberwachung, Sicherheitbereiche und Technikräume, Grundversorgung mit Strom, USV, Notstrom, Wasser, Klima sowie die technische Kommunikationsanbindung, wobei es hier thematisch Überschneidungen zu der IT-Infrastruktur gibt. Die K-Fall-Szenarien werden hier gesondert vom Risiko betrachtet und dienen als Vollständigkeits-Check für die Einschätzungen der Ebenen 2 und 3. Damit wird sichergestellt, dass mit den bestehenden

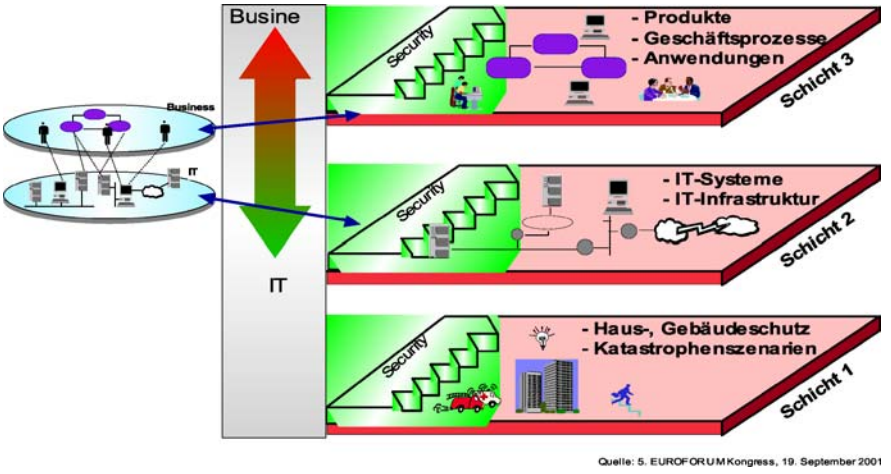


Abb. 5 Risikobetrachtung über ein Dreischichtenmodell

© Springer 2008

Ausfallvermeidungsmaßnahmen, den Notfall- und Kontinuitätsplänen, den Eskalationsverfahren sowie mit der Aufbau- und Ablaufstruktur der Krisenstäbe eine Handlungsfähigkeit gegeben ist.

- *Schicht 2* betrachtet die Risiken der den Geschäftsprozessen untergelagerten IT-Systeme und der Infrastruktur, wobei für diese Komponenten jeweils eine Schwachstellenanalyse und Risikoeinschätzung durchgeführt wird. In die Risikobetrachtung fließen die technischen Ausfallvermeidungsmaßnahmen direkt mit ein. Ebenfalls werden auch in dieser Ebene die Personal- und Rechtsrisiken implizit mit berücksichtigt. Insbesondere die Rechtsrisiken durch Outsourcing oder Auslagerung finden hier in vielen Fällen ein zusätzliches Gewicht, wobei dann alle Eventualitäten in Verträgen und SLAs genauestens geregelt sein müssen. Ziel der Risikobetrachtung in dieser 2. Ebene ist das unabhängige und frühzeitige Erkennen von Gefahrenpotential auf der Technikebene; sie dient zur Qualitätssicherung der Risikoeinschätzung von Geschäftsprozessen und Anwendungen der Ebene 3.
- *Schicht 3* betrachtet die vom Fachbereich und der Unternehmenssteuerung priorisierten Produkte. Auf dieser Basis sind zugehörige Geschäftsprozesse und Anwendungen zu identifizieren. In einem Bottom-up-Ansatz wird methodisch für jede wichtige Anwendung eine Schwachstellenanalyse und Risikoeinschätzung durchgeführt, wobei hier auch die Notfall-/Kontinuitätspläne sowie die Ausfallvermeidungsmaßnahmen mit betrachtet werden. Ebenfalls werden auch die anderen operationellen Risiken, wie Personal- und Rechtsrisiko, mit einbezogen. Bei der Ermittlung des „operationalen Risikos“ für ein Produkt/einen Prozess werden die einzelnen Risikoeinschätzungen der am Prozess beteiligten Anwendungen bewertet und in ein Ampelmodell überführt. Ebenfalls werden über die Einzeleinschätzung der am Prozess beteiligten Anwendungen eine Ausfallwahrscheinlichkeit und ein mögliches Schadenpotenzial für das Produkt bzw. den Prozess ermittelt. Auf Basis der ermittelten Informationen pro Produkt/Prozess kann der „Interne Bemessungssatz zur Bestimmung der Eigenkapitalunterlegung für operationale Risiken“, wie er im Strategiepapier von Basel II beschrieben ist, angewandt werden, wenn es sich bei dem Unternehmen um eine Bank handelt. Auf die Methode und Vorgehensweise wird an entsprechender Stelle detaillierter eingegangen.

4.2 Welche Sicherheit ist angemessen?

In den Fällen, wo durch Gesetz, Gerichtsurteile oder durch Empfehlungen von Aufsichtsbehörden Sicherheitsanforderungen ohne Interpretations- und Auslegungsspielraum vorgegeben werden, sind diese entsprechend umzusetzen und einzuhalten. In Fällen mit Interpretations- und Auslegungsspielraum sind betriebswirtschaftlich vertretbare und gängige Sicherheitsmaßnahmen vorzusehen.

Ebenfalls gilt es Sicherheitsmaßnahmen an den Stellen zu installieren, wo aus Eigeninteresse und Schutzbedürftigkeit das Unternehmen selbst Interesse an einer Vorsorge hat (z. B. Hackerangriffe, Sabotage, Spionage).

Es ist aber in allen Fällen die bestehende Grundsicherheit (USV, Notstrom, Gebäudeschutz, Sicherheitsbereiche, Überwachung, etc.) in die darüber hinausgehenden Ausfallvermeidungsmaßnahmen, Notfall- und Kontinuitätskonzepte mit einzubeziehen, um eine Überversorgung mit IT-Sicherheit sowie Notfall- und Kontinuitätsmaßnahmen zu vermeiden.

Bezogen auf das Schichtenmodell gilt für Schicht 1 die Grundsicherheit als ausreichend, falls nicht Gründe für zusätzliche Maßnahmen sprechen. Für Schicht 2 greifen ebenfalls Maßnahmen aus der Grundsicherheit (USV, Notstrom) und es sind als Minimum mindestens Datensicherungsverfahren und Zugriffsschutz zu gewährleisten; bei Systemen und IT-Infrastruktur, die die wichtigen Prozesse unterstützen, sind zusätzliche Ausfallvermeidungsmaßnahmen, wie Doppelung, Spiegelung, n+1-Technik, Ersatzteile, etc., vorzusehen. Für Schicht 3 sind Datensicherungs- und Recoveryverfahren als Standard ausreichend. Bei wichtigen (Kern-)Prozessen und Anwendungen sind Notfall- und Kontinuitätspläne unbedingt erforderlich.

In allen Fällen ist zu dokumentieren, welche und warum gerade diese Sicherheitsmaßnahmen installiert wurden, und es ist zu dokumentieren, welche (offensichtlichen) Sicherheitsmaßnahmen aus welchen Gründen nicht implementiert wurden.

4.3 Grobe Vorgehensweise für ein Risikomanagement

4.3.1 Das „operationale Risiko“

Unter Anwendung des Verfahrens zur Ermittlung des operationalen Risikos werden pro Produkt/Prozess jeweils das Risiko, die Ausfallwahrscheinlichkeit und der Schadensverlauf ermittelt. Hierzu wird das Schichtenmodell genutzt, wobei bei der Risikobetrachtung auf Produkt-/Prozessebene (Schicht 3) indirekt auch die Risiken aus der IT-Infrastruktur, Gebäudesicherheit sowie Personal-, Rechts-, und Reputationsrisiken mit einbezogen werden. Auf dieser Basis können dann beispielsweise bei einer Bank die Ermittlung der Eigenkapitalunterlegung für operationale Risiken je Produkt, je Geschäftsfeld und Geschäftsbereich gebildet werden. Diese Informationen fließen dann in eine Gesamtrisikobetrachtung als Basis zur Unternehmensrisikosteuerung mit ein.

4.3.2 Aktualisierung der Werte des operationalen Risikos

Mit jedem Change von Geschäftsprozessen, Anwendungen, Systemen und IT-Infrastruktur ist zu prüfen, ob sich das operationale Risiko geändert hat; gegebenenfalls

sind die Risikoveränderungen zeitnah in das Risikomodell einzuarbeiten. Zu Changes gehören nicht nur Veränderungen (z. B. neue Releases), sondern neue und auch ausgemusterte IT-Komponenten und Anwendungen sowie Umorganisationen, Veränderung von Zuständigkeiten, Kündigungen von so genannten Keyplayern und rechtliche und gesellschaftliche Veränderungen.

Ebenfalls führen bei tatsächlich aufgetretenen Notfällen erkannte Schwachstellen zur neuen Bewertung des Risikos.

4.3.3 Rollierender Report „Operationales Risiko“

Monatlich oder mindestens zu jedem Quartalsende ist eine Übersicht über die operationalen Risiken zu erstellen. In dieser Übersicht sind die einzelnen Produkte/-Anwendungen bzgl. der Risikoeinschätzung dargestellt, wobei folgende Indikatoren aufgeführt werden:

- Ausfallwahrscheinlichkeit des Produktes/Prozesses
- Einschätzung des Schadenpotenzials pro Produkt
- Eigenkapitalhinterlegung nach dem internen Bemessungssatz (bei Banken)
- Darstellung des erkannten Gefährdungspotentials
- Geplante Maßnahmen

Auf der Ebene der Geschäftsfelder und Geschäftsbereiche können bei Finanzinstituten die Einzelwerte der Eigenkapitalhinterlegung je Produkt aggregiert werden. Ebenfalls werden die Werte des vorhergehenden IT-Risiko-Berichtes mit aufgeführt, um Veränderungen darzustellen.

Ergänzend werden Kommentare und Empfehlungen seitens der zuständigen Funktion, wie z. B. vom Security-Officer, hinzugefügt, um einerseits auf Gefahren hinzuweisen und andererseits auch Maßnahmen zur Verringerung des operationalen Risikos zu initiieren.

4.4 Rahmen für Risikoeinschätzung operationaler Risiken

4.4.1 Definitionen

Zum Verständnis sind nachfolgend die notwendigen Definitionen aufgeführt.

a) Notfall (Katastrophenfall)

Ein Notfall ist dann eingetreten, wenn das Tagesgeschäft des Unternehmens derart beeinflusst wird, dass keine oder nur eine stark eingeschränkte Geschäftstätigkeit

möglich ist und damit ein nicht vertretbarer und verkraftbarer monetärer Schaden beim Unternehmen oder auch bei dessen Geschäftspartnern entsteht.

b) Störung

Eine Störung ist ein Zustand, der infolge eines überraschenden und außerordentlichen Ereignisses auf die Geschäftstätigkeit negativ einwirkt. Der Zustand kann mit den vorhandenen Mitteln und Kompetenzen und mit der bestehenden Aufbau- und Ablauforganisation bewältigt werden.

c) Risiko (risk)

Risiko ist die Wahrscheinlichkeit einer Bedrohung oder die relative Häufigkeit eines Schadenereignisses unter Einbezug der potenziellen Schadenshöhe.

Risiko nach DIN VDE Norm 3100 wird wie folgt definiert:

- Bei Schadensfall zu erwartendes Schadensausmaß;
- Zu erwartende Häufigkeit eines gefährdenden Ereignisses.

d) Vertraulichkeit (confidentiality)

Vertraulich sind Informationen immer dann, wenn sie nur einem eingeschränkten Kreis von Berechtigten zugänglich gemacht werden dürfen.

e) Integrität (integrity)

Integrität ist das Maß für die Korrektheit und Vollständigkeit von Daten. Integer bedeutet, dass nur erlaubte und beabsichtigte Veränderungen an Informationen zugelassen und möglich sind.

f) Verfügbarkeit (availability)

Verfügbarkeit ist die Fähigkeit, auf bestimmte Informationen in zugesicherter Form und Qualität innerhalb eines definierten Zeitraums am vorgegebenen Ort zugreifen zu können.

g) Verbindlichkeit (non repudiation)

Verbindlichkeit ist die Sicherstellung der Identität eines Kommunikationspartners bzw. die Sicherstellung der Urheberschaft.

h) Authentizität (authenticity)

Unter Authentizität ist die Echtheit und Glaubwürdigkeit einer Anwendung oder von Daten zu verstehen, die anhand der eindeutigen Identität und der sie charakterisierenden Eigenschaft überprüfbar ist (z. B. Benutzerkennung, Passwörter, …).

4.4.2 Schutzbedürftigkeitsskalen

Die Schutzwürdigkeit der zu verarbeitenden Informationen und Daten wird aus verschiedenen Blickpunkten betrachtet und bewertet.

Vertraulichkeit

Die Bewertung der Vertraulichkeit der zu verarbeitenden Informationen wird wie in der folgenden Tabelle 1 dargestellt vorgenommen:

Tabelle 1 Skalenwerte „Vertraulichkeit“

C1	Die Anwendung und/oder Daten unterliegen keinerlei Vertraulichkeitsanforderungen und können ohne Verstoß gegen Vorschriften/Gesetze und ohne andere negative Auswirkungen jedem zur Kenntnis gelangen.
C2	Der Zugriff auf Anwendungen und/oder Daten ist auf Mitarbeiter und andere befugte Stellen beschränkt. Der Verlust der Vertraulichkeit führt nur zu geringfügigen Schäden.
C3	Über diese Anwendungen und/oder Daten wird der Zugriff auf interne vertrauliche Informationen ermöglicht, wobei der Zugriff nach dem Need-to-know-Prinzip auf spezifische Organisationseinheiten beschränkt sein sollte. Der Verlust der Vertraulichkeit führt zu mittleren materiellen Schäden und/oder Imageverlusten.
C4	Es besteht ein Zugriff auf *streng vertrauliche* oder höchst sensitive (personenbezogene) Anwendungen und/oder Daten, die entsprechend den Vorgaben des Bundesdatenschutzgesetzes (BDSG) oder der internen Einstufung vor unberechtigter Kenntnisnahme zu schützen sind. Der Verlust der Vertraulichkeit führt zu erheblichen materiellen Schäden und/oder Imageverlusten.

Zum Schutz der Vertraulichkeit (**C2–C4**) sind insbesondere folgende geeignete Sicherheitsmaßnahmen zu nennen:

- Daten und Anwendungen, die nicht explizit klassifiziert wurden, gelten automatisch als nach **C3** eingestuft;
- Festlegung des Orts der Speicherung und Verarbeitung (etwa nur in internen Netzen oder nur auf Stand-Alone-Rechnern);
- Zutritts-, Zugangs-, Zugriffs- und Berechtigungskontrolle;
- Verwendung kryptographischer Verfahren zur Verschlüsselung sensitiver Daten und deren Transfer sowie mindestens Verschlüsselung des vertraulichen E-Mail-Verkehrs.

Folgende Maßnahmen zum Schutz der Vertraulichkeit sind in Abhängigkeit der Sensitivitätsklassen der Daten anzuwenden:

C1: Keine Maßnahmen.

C2: Daten und Anwendungen werden nur im internen Netzwerk oder nur den befugten Stellen zur Verfügung gestellt. Die Daten müssen verschlüsselt werden bei:

- der Übertragung über „non trusted"-Netze.

C3: Die Daten müssen verschlüsselt werden bei:

- Speicherung auf einem Notebook;
- Übertragung über „non trusted"-Netze.

C4: Die Daten müssen verschlüsselt werden bei:

- Speicherung auf einem Notebook;
- elektronischer Übertragung über ein Netzwerk, welches nicht der „Trusted Zone" angehört (ein „partly trusted"- oder „non trusted"-Netzwerk).

Der Zugang zu den Daten mit der Klassifizierung **C3** ist durch eine Authentisierung der zugreifenden Person zu reglementieren. Für Daten der Klasse **C4** sollte möglichst eine starke Authentisierung oder zusätzliche Schutzmaßnahmen, wie z. B. eine mehrstufige Zugangskontrolle, verwendet werden. Ferner dürfen die Daten der Klasse **C4** nur in lokalen Netzen der Trusted Zone verfügbar sein.

Integrität

Die Bewertung der Integrität der zu verarbeitenden Informationen wird wie in der folgenden Tabelle 2 dargestellt vorgenommen:

Tabelle 2 Skalenwerte „Integrität"

I1	Die Anwendung und/oder Daten unterliegen keinerlei Integritätsanforderungen. Absichtliche oder unabsichtliche Verfälschungen haben keine oder erkennbar unwesentliche Auswirkungen auf die entsprechende Aufgabenerfüllung.
I2	Verfälschung von Anwendungen und/oder Daten kann Schäden hervorrufen, die jedoch geringfügige und damit tolerierbare Beeinträchtigungen der Aufgabenerfüllung nach sich ziehen.
I3	Verfälschung von Anwendungen und/oder Daten kann Schäden mit mittlerer Beeinträchtigung der Aufgabenerfüllung und/oder Imageschäden hervorrufen, die jedoch tolerierbar sind, wenn sie schnell und zuverlässig erkannt und behoben werden.
I4	Vorsätzliche oder durch Fehlfunktion verursachte Verfälschungen von Anwendungen und/oder Daten können Schäden mit wirtschaftlicher Bedeutung bis hin zur totalen Arbeitsunfähigkeit und/oder dem Imageverlust führen und sind nach Möglichkeit zu verhindern.

Daten und Anwendungen, die nicht klassifiziert wurden, gelten automatisch als nach **I3** eingestuft. Zum Schutz von Daten und Anwendungen der Integritätsstufe

I3 und **I4** sind Maßnahmen zur Verhinderung und zum Erkennen von Integritätsverletzungen anzuwenden, wobei folgende Punkte besonders zu nennen sind:

- Verarbeitung und Speicherung der Daten nur auf dedizierten Rechnern;
- Zutritts-, Zugangs-, Zugriffs- und Berechtigungskontrolle;
- Abgleich mit Kontrolldaten;
- Verwendung redundanter Information wie z. B. Prüfsummen, Paritätsbits, Spiegelung;
- Verwendung kryptographischer Verfahren wie z. B. digitale Signatur, MAC (Message Authentication Code), Hash-Algorithmen;
- Einsatz von Virenscannern.

Bei Bedarf können diese Maßnahmen auch zum Schutz von Daten und Anwendungen der Integritätsstufe **I2** eingesetzt werden. Für Daten und Anwendungen der Integritätsstufe **I4** ist ein MAC oder die digitale Signatur einzusetzen.

Verfügbarkeit

Die Bewertung der Verfügbarkeit der zu verarbeitenden Informationen wird wie in der folgenden Tabelle 3 dargestellt vorgenommen:

Tabelle 3 Skalenwerte „Verfügbarkeit“

A1	Die Anwendung und/oder Daten unterliegen keinen nennenswerten Verfügbarkeits-Anforderungen. Ein längerfristiger Ausfall hat keinerlei negative Auswirkungen auf die Aufgabenerfüllung.
A2	Die Verarbeitung der Daten lässt sich um einige Tage verschieben bzw. ist während dieser Zeit manuell durchführbar und/oder Datenverluste sind ohne größeren Aufwand rekonstruierbar.
A3	Ein Ausfall der Anwendung und die Nichtverfügbarkeit von Daten sind bis zu einem Tag tolerierbar, ohne dass unaufholbare Arbeitsrückstände entstehen; Datenverluste sind nur mit großem Aufwand rekonstruierbar.
A4	Die Anwendung und Daten müssen zur Aufgabenerfüllung durchgehend zur Verfügung stehen. Ein Ausfall der Anwendung und/oder Datenverluste sind unter keinen Umständen tolerierbar.

Daten und Anwendungen, die nicht explizit klassifiziert wurden, gelten automatisch als nach **A3** eingestuft. Darüber hinaus sind folgende Schutzmaßnahmen zu nennen:

- Redundante Systeme;
- Vorhaltung von Ersatzteilen/Ersatzsystemen;
- Datenspiegelung;
- Backup der Daten;
- Überwachung.

Als Anhaltspunkt für die jeweilige Verfügbarkeit können folgende Werte vorgegeben werden:

A1: Die Verfügbarkeit pro Jahr soll mindestens bei 90% liegen und ein Einzelausfall sollte nicht länger als 5 Arbeitstage dauern.

A2: Die Verfügbarkeit pro Jahr soll mindestens bei 95% liegen und ein Einzelausfall sollte nicht länger als 3 Arbeitstage dauern.

A3: Die Verfügbarkeit pro Jahr soll mindestens bei 98% liegen und der Einzelausfall sollte maximal 8 Std. an einem Arbeitstag nicht überschreiten.

A4: Die Verfügbarkeit pro Jahr soll mindestens bei 99,5% liegen und ein Einzelausfall nach Möglichkeit zwei Stunden, maximal aber vier Stunden an einem Arbeitstag nicht überschreiten.

Verbindlichkeit

Die Bewertung der „Verbindlichkeit" der zu verarbeitenden Informationen wird wie in der folgenden Tabelle 4 dargestellt vorgenommen:

Tabelle 4 Skalenwerte „Verbindlichkeit"

B1	Die Anwendungen und Daten unterliegen keinen Verbindlichkeitsanforderungen. Schäden werden nicht erwartet.
B2	Dadurch, dass die Authentizität von Systemnutzern und von Rechnern, die Echtheit übermittelter Daten, die Einhaltung von Übermittlungswegen oder Sende- und Empfangsnachweise nicht verbindlich feststellbar und Dritten gegenüber beweisbar sind, können nur geringe, tolerierbare Schäden entstehen.
B3	Dadurch, dass die Authentizität von Systemnutzern und von Rechnern, die Echtheit übermittelter Daten, die Einhaltung von Übermittlungswegen oder Sende- und Empfangsnachweise nicht unmittelbar verbindlich feststellbar und Dritten gegenüber beweisbar sind, können größere Schäden entstehen.
B4	Die Authentizität von Systemnutzern und von Rechnern, die Echtheit übermittelter Daten, die Einhaltung von Übermittlungswegen oder Sende- und Empfangsnachweise müssen rechtsverbindlich feststellbar und Dritten gegenüber beweisbar sein. Andernfalls kann es zu massiven Schäden kommen.

Daten und Anwendungen, die nicht explizit klassifiziert wurden, gelten automatisch als nach **B3** eingestuft.

Zum Schutz der Verbindlichkeit/Authentizität (**B2–B3**) sind geeignete Sicherheitsmaßnahmen zu treffen, wobei insbesondere folgende zu nennen sind:

- Festlegung des Orts der Speicherung und Verarbeitung (etwa nur in internen Netzen oder nur auf Stand-Alone-Rechnern);
- Zutritts-, Zugangs-, Zugriffs- und Berechtigungskontrolle;

- Protokollierung von Benutzeraktionen;
- Empfangsbestätigung, Quittierung (z. B. per Email oder über andere Kommunikationswege);
- Kryptographische Verfahren zur Authentisierung und Gewährleistung der Integrität, wie Digitale Signatur oder Message Authentication Code (MAC).

Verbindlichkeit nach **B4** kann beispielsweise mit Hilfe der Digitalen Signatur erreicht werden. Dabei muss sichergestellt sein, dass es eine vertrauenswürdige Instanz gibt, die private Schlüssel zweifelsfrei zertifiziert.

4.4.3 Feststellung des Schutzbedarfs

Anhand der Skalenwerte Vertraulichkeit (C1–C4), Integrität (I1–I4), Verfügbarkeit (A1–A4) und Verbindlichkeit (B1–B4) wird der Schutzbedarf wie folgt ermittelt:

$$S_n = (C_i\ I_j\ A_k\ B_l)\ i, j, k, l \in \{1,2,3,4\} \qquad n = \max(i, j, k, l)$$

Die Schutzklasse ergibt sich aus der Maximaleinstufung der Einzelklassifizierungen. Dies bedeutet, falls eine Anwendung mit C1, I1, A3 und B1 klassifiziert wird, so ist die Schutzklasse aufgrund von A3 (Maximaleinstufung) mit S3 festzulegen. Folglich sind die entsprechenden Maßnahmen für die Schutzklasse S3 zu berücksichtigen.

Die Einstufung von Anwendungen, Daten und Dienstleistungen ist bei neu zu erstellenden Anwendungen oder Dienstleistungen vom jeweiligen zuständigen Projekt mit zu erarbeiten. Für vorhandene Anwendungen und Dienstleistungen ist der fachlich Verantwortliche (Owner) für die Durchführung der Schutzbedarfsfeststellung zuständig. Anwendungen und Daten, die nicht explizit klassifiziert wurden, werden automatisch nach S3 (interne Geschäftsdaten) eingestuft.

4.4.4 Qualitative Risikoeinschätzung einzelner Produkte

Zur qualitativen Risikoeinschätzung von Produkten wird der Prozess in einer einfachen Form pro Produkt betrachtet. Der Prozess wird in Teilschritte untergliedert, so dass jedem Teilschritt eine Anwendung oder eine Funktion zugeordnet ist (siehe Abb. 6). Da es sich hier nicht um eine standardmäßige Geschäftsprozessdarstellung mit der entsprechenden Detaillierungstiefe handelt, denn die ist für eine Risikobetrachtung zu aufwendig oder sogar zu komplex, wird eine einfache Darstellung der Aneinanderreihung der Anwendungen (Prozesskette) gewählt.

Beispielsweise können die Teilschritte der Prozesskette im Bankenumfeld wie folgt aussehen:

Handel:
1. Info
2. Pricing
3. Geschäftsabschluss
4. Geschäftserfassung
5. Positionsführung
6. Risikoüberwachung
7. Geschäftsabwicklung
8. Buchung
9. Meldewesen

Kredit:
1. Aquise
2. Info/Auswertung
3. Risikoanalyse
4. Kreditvorlage
5. Genehmigung
6. Vertragsbearbeitung
7. Valutierung
8. Abwicklung

Zahlungsverkehr:
1. Zahlungseingang
2. Scannen/OCR
3. Risikoprüfung
4. Verbuchung
5. Clearing
6. SWIFT
7. Abstimmung

Abb. 6 Aufbau der Produkt-/Geschäftsprozessketten

Aufbauend auf diese Prozessketten können nun auf Produktebenen jeweils der Schutzbedarf ermittelt und Risikoanalysen durchgeführt werden, wobei als Ansatz auch die FMEA-Methode mit den RPZs (Risikoprioritätszahlen) einsetzbar ist.

Die in einer Prozesskette festgestellten Einzelrisiken werden zur Ermittlung des Produktrisikos herangezogen und im Gesamtkontext bewertet (siehe Abb. 7). In den Fällen, wo für eine Anwendung/einen Teilprozessschritt mehrere Einzelrisiken vorliegen, sind diese ebenfalls zu konsolidieren und in der Gesamtheit zu bewerten. Das Ergebnis jeder einzelnen Bewertung wird in ein Ampelmodell überführt, wobei die Farben folgende Bedeutung haben:

Rot: Auf Basis der Risikoeinschätzung besteht für diese Anwendung bzw. für diesen Teilprozessschritt ein unmittelbarer Handlungsbedarf. Zur Risikominimierung und zur Stabilisierung sind unverzüglich Maßnahmen einzuleiten und umzusetzen.

Orange: Für diese Anwendung, für diesen Teilprozessschritt besteht auf Basis der Risikoeinschätzung ein hoher Handlungsbedarf. Maßnahmen sind zügig einzuleiten.

Gelb: Die Risikoeinschätzung zeigt einen Handlungsbedarf, mögliche Maßnahmen zur Risikoreduzierung stehen nicht unter einem zeitlichen Umsetzungsdruck oder es werden bewusst Risiken ohne Gegenmaßnahmen toleriert und eingegangen.

Grün: Die Risikoeinschätzung zeigt keinen Handlungsbedarf.

Bei der Bewertung und insbesondere auch bei geplanten Maßnahmen zur Risikominimierung ist der Kosten-/Nutzen-Aspekt mit einzubeziehen; d. h. es ist zu prüfen, welche Maßnahmen unbedingt nötig sind und welches Risiko vertretbar getragen werden kann. Nachdem die Ampel je Teilprozessschritt bestimmt wurde, kann die Einschätzung des Produktrisikos vorgenommen werden, indem die Ampel mit dem höchsten Risiko in der Prozesskette auch die Farbe der Ampel für das Produktrisiko bestimmt.

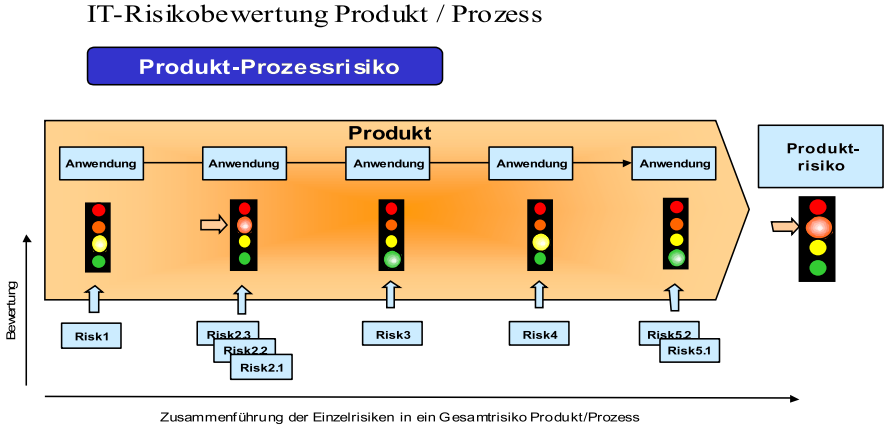


Abb. 7 Qualitative Bewertung des Produkt-/Prozessrisikos

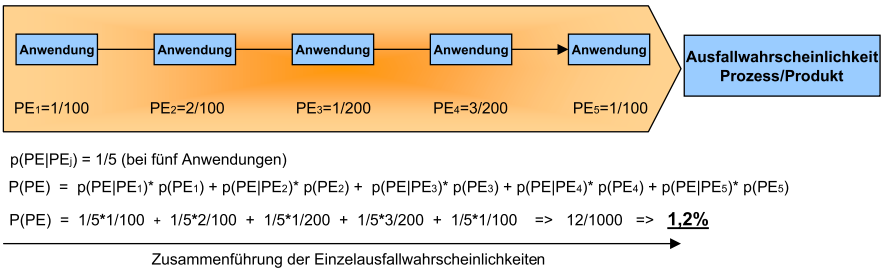


Abb. 8 Ermittlung der Ausfallwahrscheinlichkeit auf Prozessebene

Des Weiteren ist ein Parameter für die Wahrscheinlichkeit des Schadenfalls (Probability of loss event „PE“) für das IT-Risiko zu ermitteln. Zur Ermittlung der Ausfallwahrscheinlichkeit des Produktes/Prozesses wird die „Formel der totalen Wahrscheinlichkeit“ genutzt (siehe Abb. 8). Für p(PE|PEj) wird jeweils 1/Anzahl Anwendung und für p(PEj) die Ausfallwahrscheinlichkeit gesetzt.

$$p(PE) = \sum_{j=1}^{n} p(PE|PEj) * p(PEj)$$

Zur Verfeinerung des Modells kann jedem Teilprozessschritt eine Gewichtung zugeordnet werden.

Bei der Risikobetrachtung wird der Zeitpunkt, zu dem der operationale Krisenstab aktiviert wird, für die Festlegung der Auftrittswahrscheinlichkeit genommen. Der Grund hierfür ist, dass in solchen Not- und K-Fällen tatsächlich Gefahr im Verzug ist und mit Schäden zu rechnen ist. Alle Störungen und Ausfälle, die vor diesem Zeitpunkt liegen, werden im Rahmen der normalen Kompetenz und mit der bestehenden Aufbau- und Ablauforganisation bewältigt und somit nicht berücksichtigt.

Die Bewertungen und Einschätzungen sollten, wenn kein gesichertes Zahlenmaterial vorliegt, unbedingt als Expertenschätzung durchgeführt werden. Zu diesem Expertenteam gehören mindestens der verantwortliche FB sowie der Anwendungs- und Systembetreuer. Ergänzt werden kann das Expertenteam von erfahrenen Revisoren, von Wirtschaftsprüfern oder von sonstigen Personen, die Risiken einschätzen können.

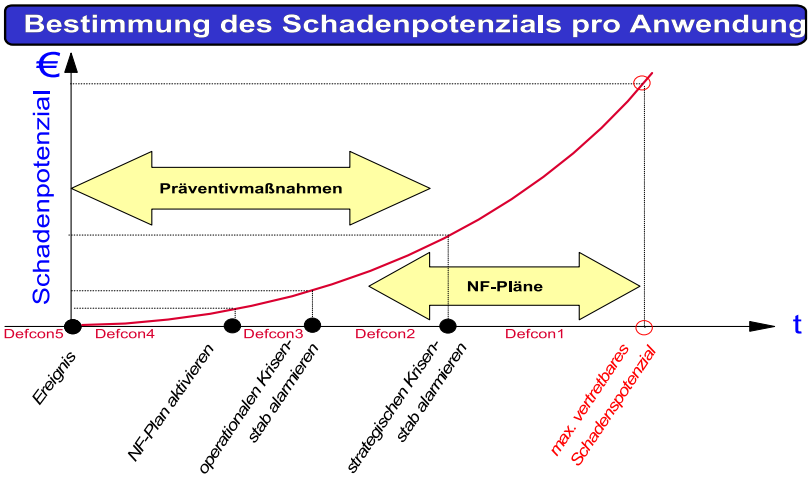
Die Experten sitzen zusammen und geben jeweils für sich selbst eine Risikoeinschätzung ab. Das Ergebnis wird in der Runde diskutiert und verifiziert. Danach wird gemeinsam die Risikoeinschätzung festgelegt, wobei entweder jeder Teilnehmer noch einmal die Risikoeinschätzung neu abgibt und dann das arithmetische Mittel gebildet wird, oder in einem gemeinsamen Konsens das Risiko festgelegt wird.

4.4.5 *Quantitative Risikoeinschätzung eines Produktes*

Zur Ermittlung des quantitativen Risikos für ein Produkt wird vom Prozess ausgegangen, wobei für jede Anwendung ein Schadensverlaufsdiagramm auf Basis der Ausfallzeiten der Notfall- und Kontinuitätsplanung erstellt wird (siehe Abb. 9).

Zur Einschätzung des monetären Schadens sind nach Möglichkeit bekannte Werte von Schadensverläufen zu verwenden, bzw. die vorgegebenen Werte aus dem Notfall- und Kontinuitätsplan zu verwenden. Sind diese Werte nicht vorhanden, so kann vom Produkt selbst oder von einem vergleichbaren Produkt der DB (Deckungsbeitrag) des Vorjahres als Basis genommen und der fiktive Schadensverlauf für entsprechend zu betrachtende Ausfallzeiten ermittelt werden.

- Der erste Wert ist die Zeit, die unmittelbar nach dem Eintreten des Notfalls bis zur Aktivierung des Notfall- und Kontinuitätsplans vergeht (z. B. die ersten zwei Std.).
- Der zweite Wert bezieht sich auf die Zeit bis zur Alarmierung des operativen Krisenstabs (z. B. nach 4 Std.), der vorgesehene Maßnahmen einleitet und im Rahmen seiner Kompetenzen Entscheidungen herbeiführt; der operative Krisenstab wird durch vorgesehene Krisenmanager, tangierte Bereichsleiter und weitere Spezialisten (Keyplayer) gebildet.
- Der dritte Wert bezieht sich auf die Zeit bis zur Alarmierung des strategischen Krisenstabs (z. B. nach einem Tag), der für notwendige strategische Entscheidungen zuständig ist; der strategische Krisenstab wird in der Regel durch die Geschäftsführung besetzt.



Bestimmung des maximal zu vertretenden Schadenpotenzial pro Anwendung/Teilprozessschritt, wobei die Höhe des Schadens und die Zeitdauer vorzugeben sind.

Abb. 9 Schadenpotenzial-/Zeit-Diagramm

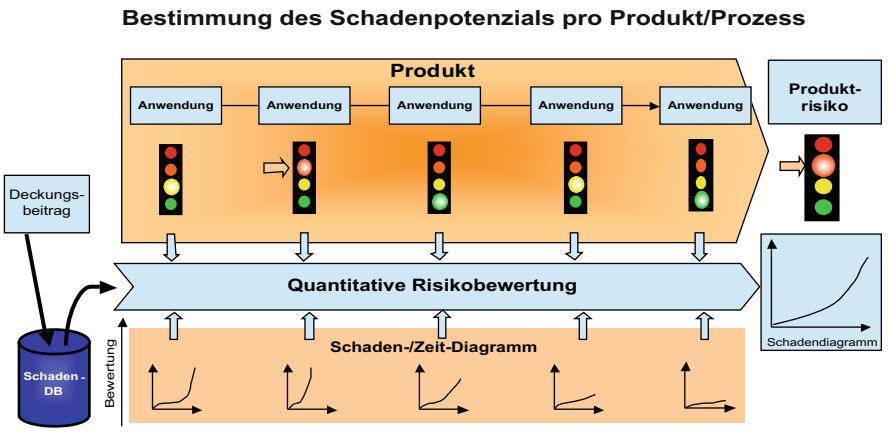


Abb. 10 Quantitative Bewertung des Produkt-/Prozessrisikos (Schadendiagramm)

- Der vierte Wert bezieht sich auf das maximal zu vertretende Schadenspotenzial, wobei die Höhe des Schadens und die Zeitdauer bis zu diesem Schaden vorzugeben sind.

Ebenfalls sind in dem Diagramm die entsprechenden Alarmstufen (Defcon = Defence Condition) aufgeführt, die sich entsprechend zwischen Defcon-5 (Normalzustand, keine Störung) und Defcon-1 (unmittelbare Gefahr für das Unternehmen) bewegen.

Auf Basis der Schadensverläufe der einzelnen Anwendungen kann nun der Schadensverlauf für ein Produkt ermittelt werden, wobei der Mittelwert aus den einzelnen Teilprozessschritten gebildet wird. Das Ergebnis ist ein Schadenpotenzial-/Zeit-Diagramm für das jeweilige Produkt (siehe Abb. 10).

Als eine weitere Stufe und zur Verfeinerung des Modells können die einzelnen Teilprozessschritte anhand ihrer Wichtigkeit und anhand ihres Schadenpotenzials entsprechend gewichtet werden.

4.4.6 Steuerung der operationalen Risiken

Aufbauend auf eine Risikoanalyse ist das Risiko (R1–R4) zu ermitteln, indem der Ist-Zustand (Risikovorsorge und -vermeidung) dem Soll-Zustand (notwendiger Schutzbedarf) gegenübergestellt wird. Bei der Überführung in das Ampelmodell wird das Risiko farblich erkennbar, wobei die Farben folgende Bedeutung haben:

- Risiko R4 (rot) = unmittelbarer Handlungsbedarf
- Risiko R3 (orange) = Handlungsbedarf
- Risiko R2 (gelb) = möglicher Handlungsbedarf, Risiko ist tragbar
- Risiko R1 (grün) = kein Handlungsbedarf

Das festgestellte Risiko ist anhand folgender Fragestellungen weiter anzupassen, wobei eine farbliche Umstufung im Gesamtkontext zu bewerten und entsprechend im Reporting aufzuzeigen ist:

- Ist der Zeitpunkt für eine regelmäßig vorgesehene Notfallübung oder Überprüfung von Präventiv- und Ausfallvermeidungsmaßnahmen mehr als 3 Monate überschritten, so ist das Risiko farblich höher einzustufen. Ist dieser Zeitpunkt um mehr als ein Jahr überschritten, so ist das Risiko farblich um eine weitere Stufe zu erhöhen (Alterung).
- Weiterhin ist die Aktualität der Dokumente, SLAs und insbesondere die Zuständigkeit bei den Schutzbedarfsklassen S3 und S4 sicherzustellen (Überprüfung einmal pro Jahr). Bei Unvollständigkeit und fehlender Aktualität kann hier das Risiko ebenfalls farblich höher eingestuft werden.
- Ist das Know-how für Prozesse oder Anwendungen personenbezogen oder besteht eine starke externe Abhängigkeit, so kann ebenfalls eine farbliche Umstufung vorgenommen werden.

4.4.7 Aufbau des Reporting mit Darstellung der Risiken auf Prozess-/Produktebene

Jeder Fachbereich hat für seine Bewertung der operationalen IT-Risiken ein Berichtswesen aufzubauen, wobei als Berichtsbasis der Geschäftsprozess oder die IT-Anwendung dient.

Tabelle 5 Monatsbericht „Operationale IT-Risiken“

<table>
<tr><td colspan="2">Geschäftsprozess/Anwendung:
Name Prozesse/Anwendungen:</td><td>Datum: TT.MM.JJJJ
Abteilung: Verantwortlicher:</td></tr>
<tr><td>Produkte:
…
…
…</td><td>Deckungsbeitrag (Jahr):
• DB1 (Rohertrag)
• DB2 (-variable Kosten)
• DB3 (-Fixkosten vor Steuer)</td><td>• Max. Ausfallzeit:
• Mögliches Schadenpotenzial bei der max. Ausfallzeit:
• Eintrittswahrscheinlichkeit</td></tr>
<tr><td colspan="3">Risiken:
• Darstellung der erkannten Risiken und deren Folgen.
• Welches Restrisiko besteht?</td></tr>
<tr><td colspan="2">Geplante und umgesetzte Maßnahmen:
• Darstellung der geplanten und noch umzusetzenden Maßnahmen zur Risikominimierung.
• Aufzeigen der umgesetzten Maßnahmen seit dem letzen Bericht zur Begrenzung oder Minimierung des Risikos.
• Wurde eine Notfallübung durchgeführt? Wann war die letzte Übung?</td><td>Durchführungsverantwortliche:

Termin:

Kosten:</td></tr>
<tr><td colspan="3">Weiterer Handlungsbedarf:
• Problemstellungen oder neue Erkenntnisse, die das Risiko erhöhen. Darstellung von Lösungen. Besteht ein Handlungs- oder Entscheidungsbedarf (Priorität, Budget, Ressourcen)?</td></tr>
</table>

Jan.	Feb.	März	April	Mai	Juni	Juli	Aug.	Sept.	Okt.	Nov.	Dez.
K3	K2	K1	K1	K1	K0	K0	K1	K1	**K0**		

Als Anleitung kann das folgende Beispiel (siehe Tabelle 5) genommen werden, wobei das Risiko anhand der Ampelfarben (rot, orange, gelb, grün) in einer Monatszeile darstellt wird. In jedem Monat wird das Risiko farblich in das vorgesehene Monatsfeld eingetragen und durch einen fetten Rahmen gekennzeichnet. Die Farben von den Vormonaten bleiben im Bericht erhalten, um Veränderungen über die Monate hinweg darzustellen.

4.4.8 Risikodarstellung der Prozesse/Anwendungen in einem Risikoportfolio

Anhand der bisherigen Einschätzung der im Fokus der Risikobetrachtung stehenden Prozesse bzw. Anwendungen werden diese entsprechend in ein Risikoportfolio eingetragen. So wird eine Gesamtübersicht des operationalen Risikos, wie in Abb. 11 zu sehen ist, zusammengestellt.

Aus dem Portfolio ist sehr gut das Gesamtrisiko zu erkennen und es können sehr einfach die entsprechenden Prozesse und Anwendungen mit Handlungsbedarf identifiziert werden.

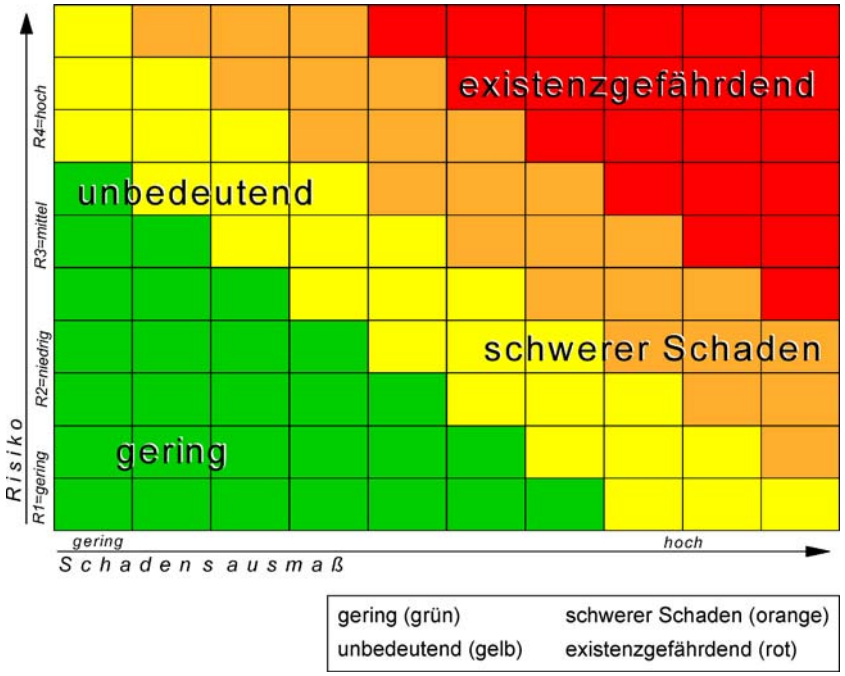


Abb. 11 Risikoportfolio der operationalen Risiken

4.4.9 Risikobewältigungsstrategien

Ein Unternehmen ganz ohne Risiko ist in der Realität nicht denkbar. Es genügt aber nicht, Risiken nur zu analysieren. Es müssen auch geeignete Maßnahmen unter betriebswirtschaftlichen Gesichtspunkten getroffen werden, die Risikoposition zu optimieren, nicht zu minimieren, weil dadurch gleichzeitig auf Gewinnchancen verzichtet würde. Grundsätzlich gibt es mehrere Strategien zum Umgang mit Risiken (Risikobewältigung):

- *Risikovermeidung* (z. B. Geschäftstätigkeit aufgrund eines nicht mehr tragbaren Risikos einstellen).
- *Risikoreduzierung*
  - ursachenbezogene Minderung der Eintrittswahrscheinlichkeit (z. B. durch redundante Auslegung von IT-Komponenten);
  - wirkungsorientierte Minderung der Schadenhöhe (z. B. Substitution fixer durch variable Kosten; Outsourcing);
  - Maßnahmen zur Schadenminderung im Eintrittsfall (z. B. Datensicherungskonzepte, Notfall-/Kontinuitäts- sowie Wiederanlaufplanung).
- *Überwälzen von Risiken* (z. B. durch Versicherung; SLAs mit Lieferanten und Dienstleistern).
- *Risiko selbst tragen* (z. B. Liquiditätsreserven zur Deckung von Schäden; Risiko-Management zur Früherkennung und Steuerung von Risiken).

Wichtig ist bei den Maßnahmen zur Risikobewältigung, jeweils einen Verantwortlichen zu benennen, notwendiges Budget und Ressourcen zur Verfügung zu stellen und mindestens einen Termin für die erfolgte Umsetzung zu vereinbaren.

4.5 Risikomanagement operationaler Risiken

Methodisch wurde die Bewertung des operationalen Risikos über die 3. Schicht (Prozess/Anwendung) durchgeführt, wobei implizit die Schicht 2 (IT-Systeme/ IT-Infrastruktur) und Schicht 1 (Gebäude, Katastrophenszenarien) mit betrachtet werden. Insbesondere sind für die 1. und 2. Schicht Risikoanalysen ebenfalls durchzuführen, die Ergebnisse werden aber in dieser Schicht nicht horizontal aggregiert und gesamtheitlich bewertet. Nur in Schicht 3 werden jeweils pro Produkt alle Risiken pro Prozessschritt/Anwendung über die Prozesskette ermittelt und dann in ein Produktrisiko zusammengeführt, wobei auch vertikal Risiken der Schichten 2 und 1 mit einfließen (siehe Abb. 12). In einem weiteren Schritt sind die entsprechend zu berücksichtigenden Katastrophenszenarien aus Schicht 1 insoweit auf Vollständigkeit der bestehenden Ausfallvermeidungen und/oder Notfall- und Kontinuitätsplanung zu prüfen, damit im entsprechenden Katastrophenfall die bestehenden oder auch geplanten Maßnahmen zur Schadenvermeidung bzw. -verminderung ebenfalls greifen.

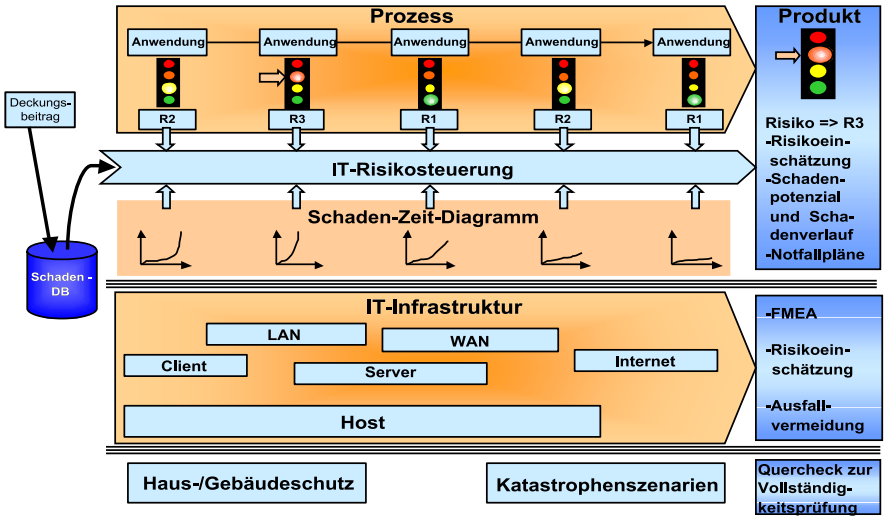


Abb. 12 Steuerung operationaler Risiken

Wie schon aufgeführt, sind diese Risikobetrachtungen und Einschätzungen keine Einmalaufgabe. Hierzu bedarf es eines permanenten Prozesses, um die Risikoeinschätzungen aktuell zu halten und entsprechende Informationen über das operationale Risiko an eine Unternehmensrisikosteuerung zu geben. Indikatoren für Risikoveränderungen der operationalen Risiken können Changeprozesse von IT-Anwendungen und Systemen, Umorganisationen, Personalweggänge oder auch externe Einflüsse, wie Gesetzesänderungen, sein. Für die Informationsgewinnung sind die entsprechenden Verfahren und Verantwortlichen zu bestimmen (von wem in welcher Form aktuelle oder veränderte Risikoinformationen zeitnah, termingerecht zu liefern sind); ebenfalls die Stelle, die die operationalen Risiken entsprechend zusammenführt und in das Risikomodell „operationale Risiken“ einpflegt. Weiterhin sind regelmäßige Reports für einen definierten Managementkreis zu erstellen.

Zur Gewährleistung einer Kontinuität und Aktualität ist der Einsatz eines Security-Officer, bei größeren Unternehmen eine Gruppe IT-Security & Contingency Management zu empfehlen. Sie sind für den Prozess „operationale IT-Risiken“ sowie für eine Aufbau- und Ablauforganisation im Not- und Krisenfall zuständig. Diese Funktion ist nach Möglichkeit direkt der Geschäftsführung zuzuordnen, damit kurze Informations- und Eskalationswege gewährleistet werden.

Des Weiteren sind in den Fachbereichen Verantwortliche für die Risikoeinschätzung, für Notfall- und Kontinuitätsmaßnahmen sowie für Notfallübungen zu benennen.

Kapitel 5
Strukturierte Risikoanalyse

Zur Bestimmung des Risikos gibt es verschiedene Verfahren und Methoden, die bei einer gleichartigen Anwendung für mehrere IT-Systeme, IT-Anwendungen und Prozesse zu aussagekräftigen Ergebnissen führen. Die im Folgenden dargestellte FMEA-Methode hat sich in der Industrie bewährt, bedeutet allerdings bei der Durchführung einen erheblichen Aufwand. Je detaillierter diese FMEA-Methode durchgeführt wird, um so genauer ist die Wahrheits- und Risikoaussage. Hier muss nun ein Maß gefunden werden, das einerseits die notwendige Tiefenschärfe gewährleistet und andererseits betriebswirtschaftlich tragbar ist. Um hier schon kurzfristig zu einem aussagekräftigen Ergebnis zu kommen, wird als erster Step ein „smart scan" vorgeschlagen. Mit Hilfe von Checklisten wird systematisch das Risiko herausgearbeitet. Danach können die Ergebnisse in die FMEA überführt und entsprechend nach und nach detailliert werden.

5.1 Schwachstellenanalyse und Risikoeinschätzung für die einzelnen IT-Systeme/Anwendungen mit der Methode FMEA

5.1.1 Übersicht

Mit der FMEA („Failure Mode and Effects Analysis" oder auch „Fehlermöglichkeits- und -einflussanalyse") werden Schwachstellenanalysen, Maßnahmen zur Beseitigung von Schwachstellen und Risikoeinschätzungen durchgeführt.

Die FMEA ist eine Methode, die Anfang der 60er Jahre in der Raumfahrttechnik entwickelt, eingesetzt und dann später auch von der Luftfahrt- und Automobilindustrie übernommen wurde. Die Methode dient dazu, bei der Entwicklung und Herstellung komplexer Produkte möglicherweise auftretende Fehler so frühzeitig

K. H. W. Thies, *Management operationaler IT- und Prozess-Risiken,*

© Springer 2008

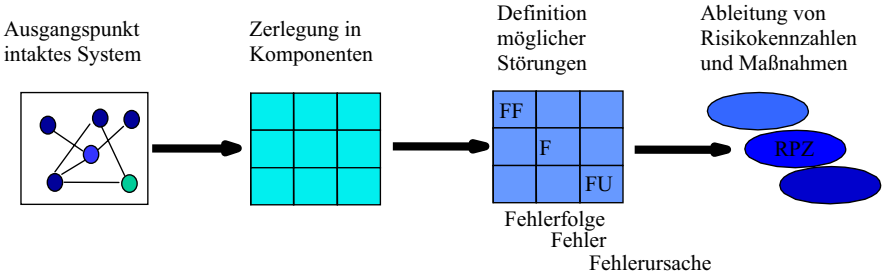


Abb. 13 Modell einer FMEA

zu erkennen, dass Fehlerverhütungsmaßnahmen wirksam werden und Fehler zurückverfolgt werden können (siehe Abb. 13).

Es wird von einem intakten System ausgegangen und dieses dann von einem übergeordneten über mehrere Stufen in untergeordnete Komponenten zerlegt. Damit ist es nun möglich, von einer fehlerhaften Komponente oder einem fehlerhaften Prozessschritt auf die untergeordneten Teilkomponenten oder Teilprozessschritte direkt zu folgern, die als Fehlerursache möglich sind. Ebenfalls ist es möglich, von der fehlerhaften Komponente oder dem Prozessschritt auf das Übergeordnete zu projizieren, auf das sich der Fehler als Fehlerfolge auswirkt. Aus den Kenntnissen und Einschätzungen der Fehlerursache, des Fehlers und der Fehlerfolge sind dann Risikoprioritätszahlen ableitbar.

5.1.2 Kurzbeschreibung der Methode

Der Aufbau einer FMEA besteht aus einer Reihe aufeinander folgender Schritte (siehe Abb. 14). Zuerst wird ein Funktionsbaum aufgestellt und der Soll-Zustand – wie funktioniert der Prozess, die Anwendung, das System? – dargestellt. Dann wird dieser Funktionsbaum in einen Fehlerbaum überführt, wobei nun die Fehlermöglichkeiten und Verzweigungen analysiert werden. Der Fehlerbaum wird im folgenden Schritt methodisch bzgl. der Fehlermöglichkeiten und Risiken gewichtet und die einzelnen Fehlerzweige priorisiert. Anhand der Priorisierung werden dann die zu untersuchenden Fehlerzweige festgelegt. In jedem Fehlerzweig werden die identifizierten Fehlerquellen hinsichtlich der Bedeutung, der Auftrittswahrscheinlichkeit und der Entdeckungswahrscheinlichkeit analysiert und bewertet (Expertenklausur), wobei bestehende Präventiv- und Ausfallvermeidungsmaßnahmen sowie vorhandene Notfall- und Kontinuitätspläne mit berücksichtigt werden.

Die Skalierung der drei Faktoren liegt zwischen 1 (niedrig) und 10 (hoch). Im Anschluss wird durch Multiplikation der drei Bewertungszahlen eine Risikoprioritätszahl (RPZ) ermittelt. Als Ergebnis zeigt die FMEA den Ist-Zustand, mögliche Fehlerquellen (Schwachstellen) und bestehende Risiken (Ist-Risiko) auf. Ist Handlungsbedarf zu erkennen, so können nun mögliche Maßnahmen zur

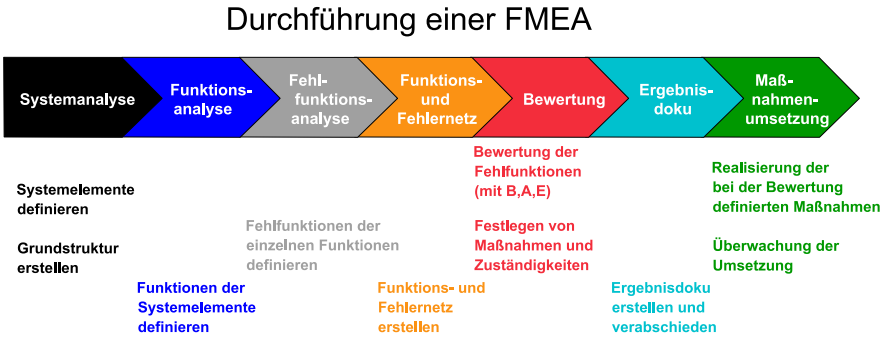


Abb. 14 Phasen einer FMEA

Schwachstellenbeseitigung in die bisherige Bewertung einbezogen und eine neue Risikoeinschätzung (Soll-Risiko) vorgenommen werden, d. h. die Methode ermöglicht eine hypothetische Risikobetrachtung und Risikoermittlung bei zusätzlichen oder geänderten Vermeidungs- oder Notfallmaßnahmen.

Werden als Ergebnis der FMEA Maßnahmen zur Risikominimierung eingeleitet, so können über diese Methode auch Termine und Verantwortlichkeiten festgelegt werden.

Der wesentliche Vorteil der FMEA ist ihre strikte Formalisierung, da systematisch mit Formblättern gearbeitet wird. Dadurch ergibt sich methodisch eine durchgängige und aussagekräftige Dokumentation der identifizierten Risiken.

5.1.3 Begriffsbestimmung

Um eine einheitliche Nutzung des Fachvokabulars sowie das entsprechende Verständnis für die Methode zu gewährleisten, werden in der folgenden Tabelle 6 die gebräuchlichsten Begriffe definiert:

Tabelle 6 Begriffsdefinitionen der FMEA

Änderungsstände	stellen den kontinuierlichen Verbesserungsprozess dar, indem sie angeben, welche Maßnahmen für eine Fehlerursache im Laufe der Zeit getroffen wurden
Entdeckungs-maßnahmen	geben an, wie Fehlerursachen entdeckt werden können (Qualitäts-sicherung)
Fehlernetz	setzt Fehlfunktionen zueinander in Beziehung; hierarchische Verkettung von Fehlfunktionen (Fehlerbaum)
Fehlfunktion	potentielle Versagensart von Funktionen
FMEA	Failure Mode and Effects Analysis

Tabelle 6 (Fortsetzung)

FMEA-Formblatt	fasst die Information über Fehlerzusammenhänge, Fehlerrisiko und eingeleitete und geplante Maßnahmen sowie deren Wirksamkeit in einem Formblatt zusammen; zeigt sämtliche Informationen zur Berechnung der RPZ
Funktion	qualitative Anforderung an das System
Funktionsnetz	setzt Funktionen zueinander in Beziehung; hierarchische Verkettung von Funktionen (Funktionsbaum)
Maßnahmengruppen	fassen Maßnahmen innerhalb eines Änderungsstandes zusammen, um so Alternativen, die diskutiert, aber nicht umgesetzt wurden, dokumentieren zu können
Risikoprioritätszahl (RPZ)	Indikator zur Messung der Schwere von Fehlern und Fehlerursachen; Produkt aus Bedeutung, Auftretens- und Entdeckungswahrscheinlichkeit
Strukturbaum	setzt Systemelemente zueinander in Beziehung
Systemelement	Bestandteile, aus denen sich die betrachteten Anwendungen zusammensetzen (Funktionen der Software)
Termine	geben an, bis wann Maßnahmen umzusetzen sind
Verantwortliche	sind für die Durchführung von Maßnahmen zuständig
FMEA-Verantwortlicher	Koordination/Unterstützung bei Initiierung, Aktualisierung und Maßnahmenumsetzung aller FMEAs
FMEA-Team	Zuständig für die Risikoeinschätzung und Bewertung; setzt sich aus „FB“, zuständigen Serviceeinheiten und weiteren Experten zusammen.
Vermeidungsmaßnahmen	geben an, wie Fehlerursachen vermieden werden können

5.1.4 Anwendung der Methode FMEA

Systemanalyse

Erster Schritt bei der Durchführung einer FMEA ist die Festlegung der Systemelemente und die damit einhergehende Erstellung der Grundstruktur (siehe Abb. 15).

Aufgrund der bisherigen Erfahrungen bei durchgeführten FMEAs sind folgende Gruppierungen und Untergruppierungen zu wählen:

- Level 1 – Geschäftsprozess, IT-Anwendung
- Level 2 – Eingabe, Verarbeitung, Ausgabe

Ab Level 3 sind die Systemelemente individuell zu identifizieren. Besonderes Augenmerk ist hierbei auf die Begrifflichkeit der „Systemelemente = Funktionen der Software“ zu legen, es darf nach Möglichkeit keine Differenzierung anhand von Organisationseinheiten, Abteilungen oder Gruppen erfolgen.

Level 4 und weitere können nach Bedarf und Notwendigkeit der Komplexität des übergeordneten Systemelements erstellt werden, d. h. es ist nicht zwingend erforderlich, dass für die gesamte Grundstruktur der gleiche Level an Tiefenschärfe erstellt wird.

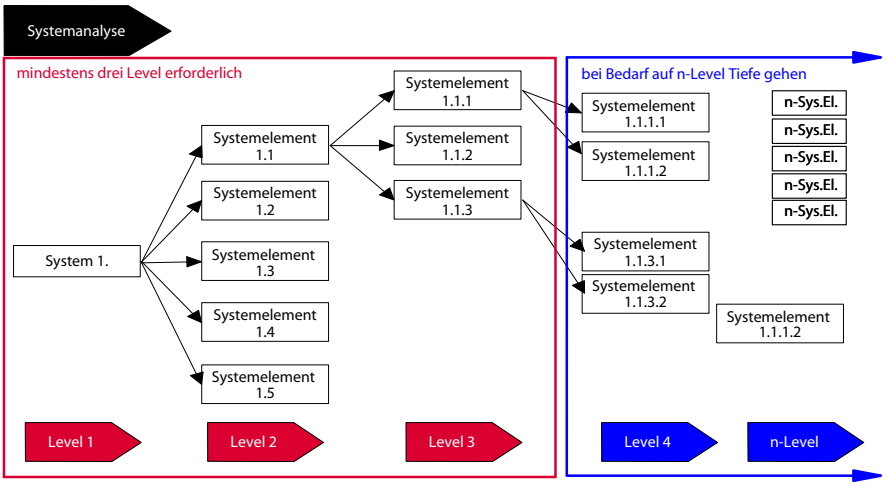


Abb. 15 FMEA-Systemanalyse

Funktionsanalyse

Nach Definition der Systemelemente und Erstellen der Grundstruktur sind für die einzelnen Systemelemente die zugehörigen Funktionen festzulegen (siehe Abb. 16). Jedem Systemelement ist mindestens eine Funktion zuzuordnen.

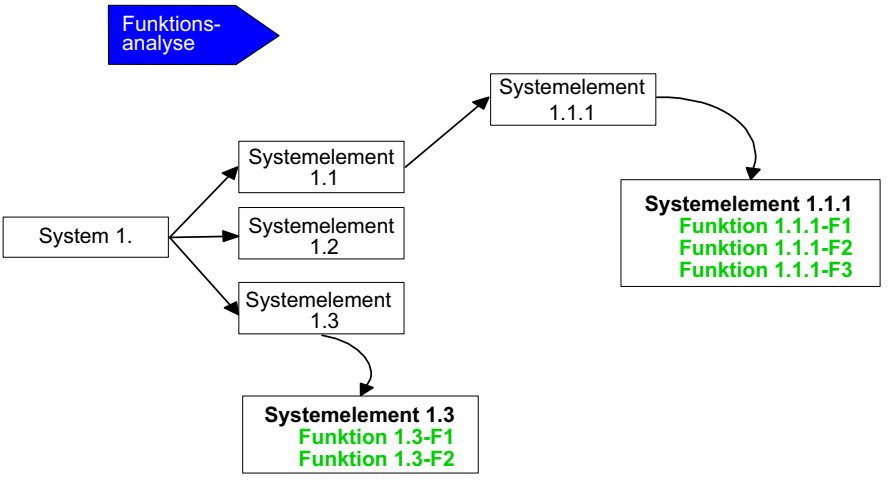


Abb. 16 FMEA-Funktionsanalyse

Fehlfunktionsanalyse

Für die festgelegten Funktionen werden dementsprechend wiederum potentielle Fehlfunktionen aufgeführt (siehe Abb. 17). Auch hier können mehrere Fehlfunktionen einer Funktion zugeordnet werden, jedoch mindestens eine ist erforderlich. Vor allem ist hierbei zu beachten, dass nicht nur die offensichtlichen und im Tagesgeschäft auftretenden Fehler, sondern alle potentiellen Fehlermöglichkeiten aufgeführt und entsprechend formuliert werden. Jeder mögliche Denkansatz ist wichtig, um die Eventualgefahren erkennen und beheben/vermeiden zu können. Bei diesem Schritt ist seitens des FMEA-Teams Kreativität, abstraktes Denken und auch der gesunde Menschenverstand erforderlich.

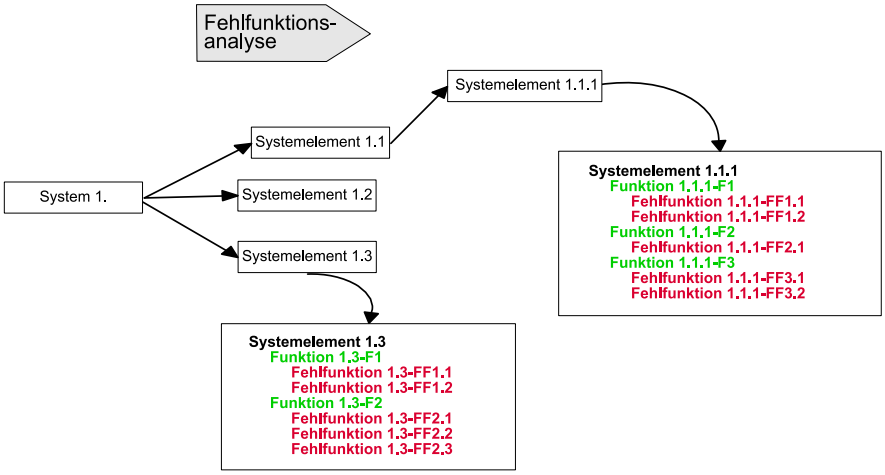


Abb. 17 FMEA-Fehlfunktionsanalyse

Funktions- und Fehlernetz

Bei der Erstellung und Verknüpfung von Funktions- wie auch Fehlernetz gilt die einfache Regel: von unten nach oben verknüpfen (rechts nach links), immer den logischen Pfad suchen und bis zum Ende durchdeklinieren (siehe Abb. 18). Jede Funktion/Fehlfunktion auf einem niedrigeren Level muss durchgängig bis zum Level 1 mit entsprechenden übergeordneten Funktionen/Fehlfunktionen verknüpft werden können. Ist dies nicht der Fall, besteht ein logischer Fehler im bisherigen systematischen Aufbau der FMEA, bzw. bei der Definition von Funktionen/Fehlfunktionen. Dieser fehlerhafte Teil ist demzufolge nochmals zu überarbeiten.

Wichtig ist hier vor allem das Fehlernetz, da dies im nächsten Schritt zur Bewertung der einzelnen Fehlfunktionen/Fehlerursachen verwendet wird.

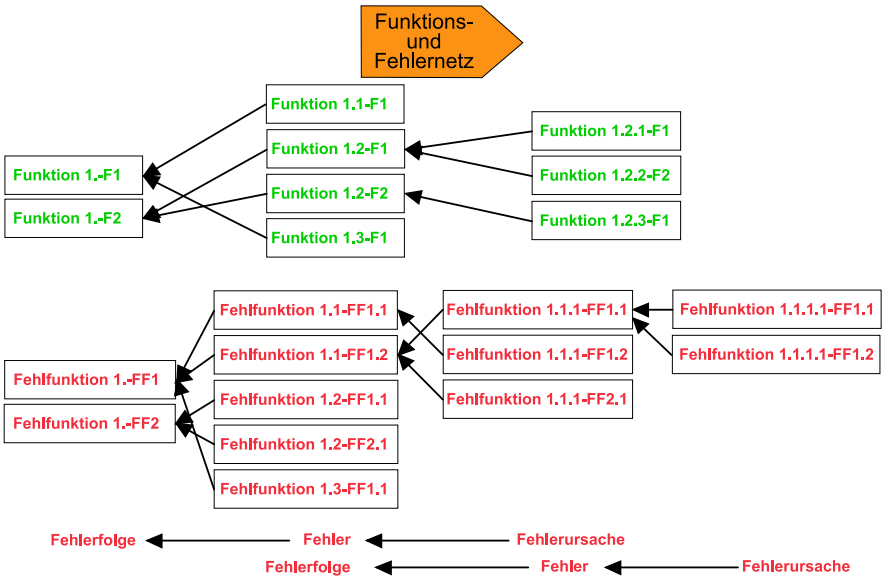


Abb. 18 FMEA-Funktions- und Fehlernetz

Gewichtung/Priorisierung innerhalb des Funktions- und Fehlernetzes

Zur Vereinfachung und Beschleunigung des Verfahrens werden alle Fehlfunktionen auf ihre Wichtigkeit und Bedeutung hin untersucht, bewertet und priorisiert (siehe Tabelle 7).

Die Priorisierung wird so vorgenommen, dass in jeder Spalte eine Fehlfunktion betrachtet wird und jede Position mit 1 = „unwichtig“, 2 = „relevant“, 3 = „zwingend erforderlich“ eingestuft wird. Danach werden in der untersten Zeile die Summen gebildet und die Fehlfunktionen mit den höchsten Summen ermittelt (priorisiert) und für die weitere, vertiefende Analyse festgelegt.

Gewichtung/Priorisierung für die einzelnen Fehlfunktionen des Prozesses und der jeweiligen Teilprozesse:

Tabelle 7 Gewichtung/Priorisierung einzelner Fehlfunktionen

Prozess:	Teilprozess:	1	2	3	4	5	6	7
Kriterien:								
Erfüllung gesetzlicher Anforderungen (z. B. KonTraG, BDSG, GoB, GoDV)								
Einhaltung Datenschutz (vertrauliche Geschäftsdaten)								
Gewährleistung der Datensicherheit (Backup, Recovery)								
Ausweichmöglichkeit durch Workaround, Notfallplan, Notarbeitsplätze								

Tabelle 7 (Fortsetzung)

Prozess:	Teilprozess:	1	2	3	4	5	6	7
Kriterien:								
Gewährleistung der physischen Sicherheit (Hardware, Räume, Zutritt)								
Beachtung allgemeiner Richtlinien (ORG-Handbuch, DIN, etc.)								
Verfügbarkeit des Prozesses und der IT-Anwendungen								
Gewährleistung der Verarbeitungsqualität, inkl. abweichendem Mengengerüst (Fehlertoleranz)								
Gewährleistung der Verarbeitungsquantität inkl. definierter Abweichungen (Durchsatz)								
Einhaltung von zeitlichen Zusagen (SLAs)								
Vermeidung von Haftung/Gewährleistung								
Schutz vor Imageschäden								
Summe:								

Spalteneintrag je Teilprozess (1 bis n):
1 = unwichtig; 2 = relevant; 3 = zwingend erforderlich

Das FMEA-Formblatt

Nachdem die weiter zu betrachtenden Fehlfunktionen herausgearbeitet wurden, wird pro Fehlfunktion ein FMEA-Arbeitsblatt angelegt (siehe Tabelle 8). Zur Darstellung des Ist-Zustandes werden in das Formular die priorisierten Fehlerursachen aus der Fehlfunktionsanalyse eingetragen. In weiteren Spalten werden entsprechend die Fehlervermeidungsmaßnahmen und die Maßnahmen zur Entdeckung von Fehlern notiert. Danach wird die Bewertung und Einstufung im

Tabelle 8 FMEA-Formblatt

	Maßnahmenbewertung Fehler-Möglichkeits- und Einfluss-Analyse								**FMEA-Nr.:** Seite von	
Funktion/Aufgabe:			**Änderungsstand:**			**Verantwortlicher:**			**Abt.:** Datum	
Mögliche Fehlerursache mit zugehörigem Fehler und Fehlerfolge	**B**	**Vermeidungs-maßnahmen**	**A**	**Entdeckungs-maßnahmen**	**E**	**RPZ**	**V / T**	**K / N**	**Realisierbarkeit**	**Prio**

B = Bewertungszahl für Bedeutung
A = Bewertungszahl für AuftrittswahrscheinlichkeitT = Termin für die Erledigung
E = Bewertungszahl für EntdeckungswahrscheinlichkeitK / N = Kosten/Nutzen
RPZ = Risikoprioritätszahl (Produkt aus B*A*E)Realisierbarkeit = Zeit, Aufwand,Verfügbarkeit
V = Verantwortlicher
Prio= 1: hoch; 2: mittel; 3:niedrig

Ergebnisse der FMEA sind ➔ Risikoeinschätzung, Maßnahmenkatalog

Tabelle 9 Skalenwert der „Bedeutung“ in der FMEA

Skalenwert der „Bedeutung“	Bewertungszahl
Sehr hoch Gesetzliche Vorschriften werden nicht eingehalten. Extrem hohes Sicherheits- und betriebswirtschaftliches Risiko für das Unternehmen. Es besteht unmittelbar Gefahr für Leib und Leben.	10–9
Hoch Funktionalitätseinschränkung wichtiger Teilsysteme. Wichtige, zugesicherte Eigenschaften können nicht genutzt werden. Der Kunde kann nur mit sehr hohem Aufwand und dann nur eingeschränkt die Funktionalität nutzen.	8–7
Mäßig Funktionalitätseinschränkung einzelner wichtiger Elemente. Grundfunktion ist nutz- und handhabbar, jedoch mit gewissem Aufwand verbunden.	6–4
Gering Funktionalitätseinschränkung einzelner weniger Elemente. Grundfunktion ist im Großen und Ganzen ohne wahrnehmbare Beeinträchtigungen verfügbar.	3–2
Sehr gering Keine Funktionalitätseinschränkungen wahrnehmbar.	1

Rahmen einer Expertenklausur vorgenommen. Anhand vorliegender Informationen, Messgrößen und Erfahrungswerte wird für jede Fehlfunktion der Faktor „B“ für die Bedeutung festgelegt (siehe Tabelle 9).

In einem zweiten Schritt wird der Faktor „A“ der Auftretenswahrscheinlichkeit des Fehlers ermittelt, wobei hier nach Möglichkeit auf bestehendes Zahlenmaterial, wie Job-Accounting, Fehlerprotokolle des UHD und Einschätzungen von Experten und Controllern zurückgegriffen werden sollte (siehe Tabelle 10).

Tabelle 10 Skalenwert der „Auftretenswahrscheinlichkeit“ in der FMEA

Skalenwert der „Auftretenswahrscheinlichkeit“	Bewertungszahl
Sehr hoch Sehr häufiges Auftreten der Fehlerursache. Die Funktionalität ist demzufolge gänzlich unbrauchbar.	10–9
Hoch Wiederholtes Auftreten der Fehlerursache. Die Funktionalität ist fast unbrauchbar, schwer kontrollierbar.	8–7
Mäßig Gelegentliches Auftreten der Fehlerursache. Die Funktionalität ist trotz offensichtlicher Mängel durchaus brauchbar.	6–4
Gering Seltenes Auftreten der Fehlerursache. Die Funktionalität ist mit minimalen Einschränkungen brauchbar.	3–2
Sehr gering Auftreten der Fehlerursache ist unwahrscheinlich.	1

Tabelle 11 Skalenwert der „Entdeckungswahrscheinlichkeit“ in der FMEA

Skalenwert der Entdeckungswahrscheinlichkeit	Bewertungszahl
Sehr gering Entdecken der aufgetretenen Fehlerursache ist unwahrscheinlich, die Fehlerursache wird oder kann nicht geprüft werden.	10–9
Gering Entdecken der aufgetretenen Fehlerursache ist weniger wahrscheinlich, die Fehlerursache wird oder kann kaum bzw. nur mit unverhältnismäßig hohem Aufwand geprüft werden.	8–7
Mäßig Entdecken der aufgetretenen Fehlerursache ist wahrscheinlich, Prüfungen sind relativ sicher.	6–4
Hoch Entdecken der aufgetretenen Fehlerursache ist sehr wahrscheinlich, Prüfungen sind sicher.	3–2
Sehr hoch Entdecken der Fehlerursache ist absolut sicher (Selbstentdecker).	1

Als dritte Größe wird der Faktor „E“ der Entdeckungswahrscheinlichkeit des Fehlers ermittelt, d. h. welche Maßnahmen bestehen, um Fehler frühzeitig zu erkennen (siehe Tabelle 11).

Bewertung

Die rechnerische Bewertung und Ermittlung der RPZ erfolgt anhand einer Multiplikation der Bewertungszahlen „Bedeutung, Auftretenswahrscheinlichkeit und Entdeckungswahrscheinlichkeit“ (siehe Abb. 19).

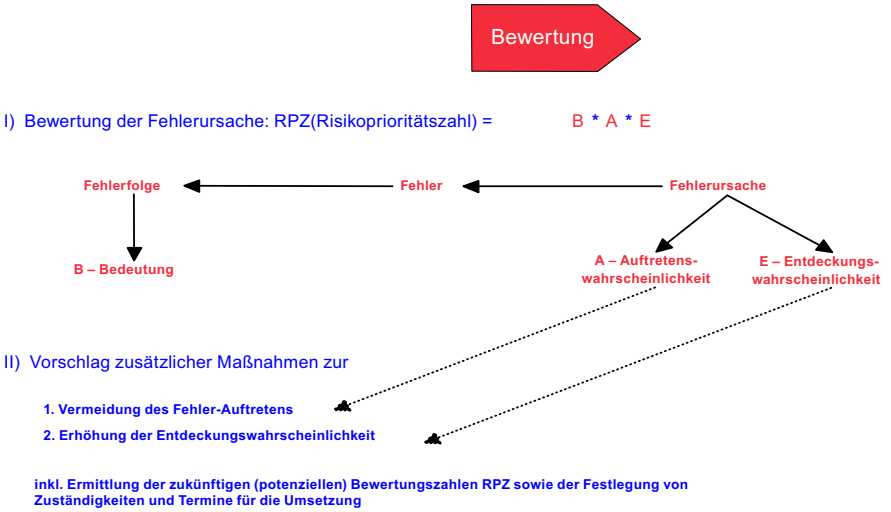


Abb. 19 Bewertung

Ermittelte RPZs können durch die Einführung neuer Vermeidungs- bzw. Entdeckungsmaßnahmen verbessert werden; in diesem Fall werden zusätzlich noch durchzuführende Vorkehrungen und Maßnahmen in das jeweilige FMEA-Formblatt unterhalb des Ist-Zustandes mit eingetragen. Auf Basis dieses zukünftigen Sachstands werden die Faktoren „A“ und „E“ neu festgelegt und die RPZ ermittelt. Die somit neu errechnete RPZ wird im FMEA-Formular (siehe Tabelle 8) in Klammern dargestellt und dient als anzustrebende Zielgröße. Den umzusetzenden Maßnahmen werden gleichzeitig „Verantwortlicher“ und „Termin“ zugeordnet, was eine Termin- und Maßnahmenkontrolle ermöglicht.

Ergebnisdokumentation

Die Ergebnisdokumentation ist i. d. R. durch den FMEA-Verantwortlichen zu erstellen und mit dem FB, den zuständigen Serviceeinheiten sowie allen betroffenen Bereichen und Organisationseinheiten abzustimmen, wobei es insbesondere auf die Nachvollziehbarkeit der Bewertung sowie die einzuleitenden Umsetzungsmaßnahmen und Termine ankommt (siehe Abb. 20).

Ergebnisdoku

Ergebnisdokumentation

Ziele:

- Logik und Vorgehensweise der durchgeführten FMEA für Außenstehende nachvollziehbar darstellen
- Klare und verständliche Dokumentationslage als Ergebnissicherung schaffen
- Grundlage für nachfolgende FMEAs bereitstellen

Inhalte:

- Kurzbeschreibung der Vorgehensweise, Schilderung aufgetretender (auch organisatorischer) Probleme
- Festhalten der Gesprächs- und Diskussionspartner, des FMEA-Teams, des FMEA-Verantwortlichen
- Kurzkommentare zu den einzelnen Fehlerursachen und, falls notwendig, Begründung zur deren Bewertung
- Erläuterung und Begründung der aufgeführten und geplanten Umsetzungsmaßnahmen für Auftretens- und Entdeckungswahrscheinlichkeit
- Anhang: Grundstruktur, Funktionsnetz, Fehlernetz, alle Formulare

Abb. 20 Ergebnisdokumentation

Maßnahmenumsetzung

Nachstehende Übersicht (siehe Abb. 21) zeigt die Aufgabenverteilung bei der Maßnahmenumsetzung und der Überwachung von Terminen, etc. Abhängig von der Aufbauorganisation sind entsprechende Verantwortung, Kompetenz und Zuständigkeit zu definieren.

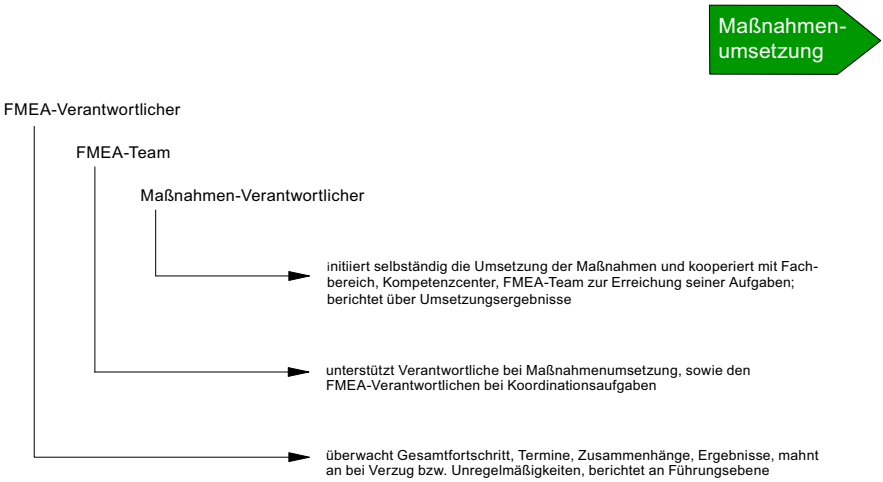


Abb. 21 Maßnahmenumsetzung

5.2 Strukturierte Risikoanalyse (smart scan)

5.2.1 Generelle Vorgehensweise

Da in vielen Fällen eine große Anzahl von Prozessen, Anwendungen und Systemen zu analysieren ist, ist für den ersten Ansatz eine grob strukturierte Kurzanalyse sinnvoll (siehe Abb. 22). Damit ist es möglich, in relativ kurzer Zeit eine erste Sicht auf die Prozesse und Anwendungen zu bekommen und auch schon gravierende Schwachstellen im ersten Ansatz zu erkennen. Auf Basis dieser Erkenntnisse können Maßnahmen vereinbart und entsprechend umgesetzt werden. Im Rahmen

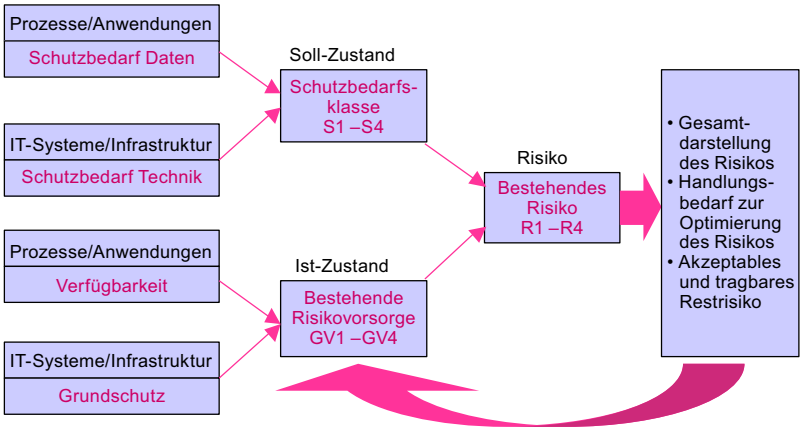


Abb. 22 Weg zur Ermittlung des operationalen IT-Risikos

einer weiteren Verbesserung der Risikoanalyse können die Checklisten in die FMEA-Methode überführt werden.

Ausgehend von dem 3-Schichten-Modell wird bei der Vorgehensweise der Soll-Zustand auf Prozess- und Anwendungsebene (Schicht 3) sowie auf der Ebene der IT-Systeme und Infrastruktur (Schicht 2) festgelegt. Des Weiteren wird dann der Ist-Zustand für die Prozess- und Anwendungsebene und für die IT-System- und Infrastrukturebene ermittelt. Im nächsten Schritt werden der Schutzbedarf (Soll-Zustand S1–S4) und die Risikovorsorge (Ist-Zustand GV1–GV4) aus den jeweiligen Einzelwerten gebildet. Auf dieser Basis werden Soll- und Ist-Zustand abgeglichen und die Differenz als Risiko (R1 bis R4) sowie entsprechende Maßnahmen herausgearbeitet.

5.2.2 Übersicht über die Klassifizierung und Einschätzung

In der folgenden Tabelle (siehe Tabelle 12) wird eine Übersicht der Klassifizierung und Einschätzung des operationalen Risikos unter Verwendung der Methode „smart scan“ dargestellt:

Tabelle 12 Übersicht Klassifizierung/Einschätzung „smart scan“

Klassifizierung und Einschätzung des Schutzbedarfs					
Schutzbedarf:	gering	niedrig	mittel	hoch	
Bewertung der Schutzbedürftigkeit (Soll-Zustand)					
Vertraulichkeit	C1	C2	C3	C4	Klassifikation
Integrität	I1	I2	I3	I4	Klassifikation
Verfügbarkeit	A1	A2	A3	A4	Klassifikation
Verbindlichkeit	B1	B2	B3	B4	Klassifikation
Schutzkl. Prozess/Anwendung	SPA1	SPA2	SPA3	SPA4	
Schutzkl. IT-Systeme/Infrastruktur	SIT1	SIT2	SIT3	SIT4	
Einschätzung des gesamten Schutzbedarfs (Soll-Zustand)					
Schutzbedarfsklasse	S1	S2	S3	S4	Klassifikation
Feststellung der bestehenden IT-Sicherheit und Notfallmaßnahmen (Ist-Zustand)					
Grundsicherheit der IT-Systeme und Infrastruktur	G1	G2	G3	G4	Ist-Zustand
Risikovorsorge/ Ausfallvermeidung von IT-Anwendungen	V1	V2	V3	V4	Ist-Zustand
Zusammenfassung der bestehenden Grundsicherheit und Risikovorsorge (Ist-Zustand))					
Gesamt Risikovorsorge	GV1	GV2	GV3	GV4	Ist-Zustand
Feststellung des bestehenden Risikos durch Vergleich der Schutzbedarfsklasse (Soll-Zustand) mit der bestehenden Gesamt-Risikovorsorge (Ist-Zustand)					
Farben:	grün	gelb	orange	rot	
Risiko	R1	R2	R3	R4	
Handlungsbedarf:	kein	optional	mittelbar	unmittelbar	

Anmerkung: Die Tabelle wird von oben nach unten bearbeitet, wobei zuerst der Schutzbedarf (Soll-Zustand) ermittelt wird. Danach wird der Ist-Zustand anhand bestehender Risikomaßnahmen festgestellt. Danach werden Soll- und Ist-Zustand zusammengeführt und das bestehende Risiko ermittelt.

Aus der Tabelle ist ersichtlich, dass sich für jeden zu untersuchenden Prozess oder Anwendung drei Kenngrößen ergeben:

- Der Schutzbedarf beschreibt den Soll-Zustand (S1–S4).
- Die Gesamt-Risikovorsorge (GV1–GV4) zeigt den Ist-Zustand bestehender Schutzmaßnahmen auf; sie umfasst die Grundsicherheit der IT-Infrastruktur und IT-Systeme sowie die Notfallvorsorge für Geschäftsprozesse und IT-Anwendungen.
- Das bestehende Risiko (R1–R4) leitet sich aus der Differenz des Schutzbedarfs (Ist) zur Gesamt-Risikovorsorge (Soll) ab und zeigt möglichen Handlungsbedarf zur Optimierung operationaler IT-Risiken auf.

5.2.3 Feststellung des Schutzbedarfs

Anhand der Skalenwerte Vertraulichkeit (C1–C4), Integrität (I1–I4), Verfügbarkeit (A1–A4) und Verbindlichkeit (B1–B4) wird der Schutzbedarf ermittelt:

$$S_n = (C_i\ I_j\ A_k\ B_l)\ \ i, j, k, l \in \{1,2,3,4\} \qquad n = \max(i, j, k, l)$$

Die Schutzklasse ergibt sich aus der Maximaleinstufung der Einzelklassifizierungen. Dies bedeutet, falls eine Anwendung mit C1, I1, A3 und B1 klassifiziert wird, so ist die Schutzklasse aufgrund von A3 (Maximaleinstufung) mit S3 festzulegen. Folglich sind die entsprechenden Maßnahmen für die Schutzklasse S3 zu berücksichtigen.

- S1: kein Schutzbedarf
- S2: geringer Schutzbedarf
- S3: mittlerer (normaler) Schutzbedarf
- S4: hoher Schutzbedarf

In einem ersten Schritt wird die Schutzbedarfsklasse Prozesse/Anwendungen festgelegt, wobei als Orientierung die entsprechende Checkliste genutzt werden kann. Zur Kennzeichnung wird der Schutzbedarf mit SPA1, SPA2, SPA3 oder SPA4 dargestellt.

In einem zweiten Schritt wird die Schutzbedarfsklasse für die IT-Systeme/ IT-Infrastruktur festgelegt. Als Hilfe und Orientierung kann die entsprechende Checkliste herangezogen werden. Zur Kennzeichnung wird diese mit SIT1, SIT2, SIT3 oder SIT4 dargestellt.

5.2.4 Checkliste Feststellung der Schutzbedarfsklasse bei Prozessen/Anwendungen

Bei der Festlegung der Schutzbedarfsklasse steht die Wichtigkeit des zu betrachtenden Prozesses oder der Anwendung im Vordergrund. In vielen Fällen haben

hier auftretende Störungen oder Ausfälle eine Außenwirkung mit möglichen Konsequenzen für das Unternehmen (Imageschaden, Haftung, Gewährleistung). Durch die unterschiedlichsten Anforderungen, die möglicherweise auch noch branchenspezifisch sind, kann hier nur ein Template (siehe Tabelle 13) vorgegeben werden, das entsprechend angepasst und ergänzt werden muss. Diese Checkliste dient einerseits dazu, die Schutzbedarfsklasse und die entsprechenden Anforderungen zu definieren und andererseits erkannte Defizite aufzuzeigen.

Die Schutzbedarfsklasse ist aus den Klassifizierungen der Vertraulichkeit, Verfügbarkeit, Verbindlichkeit und möglicherweise aus weiteren Faktoren zu bilden, wobei in der Checkliste (Tabelle 13, Spalte links) jeweils die Schutzbedürftigkeit von 1–4 klassifiziert wird oder andere Klassifizierungsmerkmale eingetragen werden. In der untersten Zeile kann dann durch die Einzelklassifizierung und durch die Berücksichtigung der zusätzlichen Klassifizierungsmerkmale die Schutzbedarfsklasse SPA festgelegt werden.

Tabelle 13 Checkliste Schutzbedarfsklasse bei Prozessen/Anwendungen

Klassifizierung 1 bis 4 oder Eintrag von Klassifizierungsmerkmalen			
	Bemerkung	Verant-wortlich	
System:	Name Prozess/Anwendung		
Bewertung: Verfügbarkeit:	Bewertung: Vertraulichkeit C1 bis C4 Integrität I1 bis I4 Verfügbarkeit A1 bis A4 Verbindlichkeit B1 bis B4 Konkretisierung der notwendigen Verfügbarkeit in %/Jahr 90%, 95%, 98%, > 99,5% Gibt es Notarbeitsplätze, wann sind diese verfügbar?		
Ausfall-verträglichkeit:	mögliche zu verkraftende Ausfallzeiten an einem Stück Ausfallzeiten, Wartung, Changes Wiederanlaufzeit Verlauf des Schadenpotenzials bei Überschreitung der verträglichen Ausfallzeiten		
Schadenpotenzial:	Welcher Schaden kann entstehen? (Umsatzverlust, Imageschäden, unmittelbare oder mittelbare Folgeschäden)		
Risiken:	Welche Risiken sind zu betrachten? (Imageschäden, unmittelbare oder mittelbare Folgeschäden, Haftungen, Gewährleistung)		
Präventiv-, Ausfall-vermeidungsmaßnahmen für Prozesse/ Anwendung	Sind Präventiv-, Ausfallvermeidungsmaßnahmen für den Prozess/Anwendung (Zettel, Handy, Notarbeitsplätze, Notfall- und Kontinuitätsplan) notwendig? Wenn nein, Begründung dokumentiert		
Notfall-, Kontinuitätspläne	Notfallpläne, Workarounds vorhanden, regelmäßig getestet? Bestehen Notarbeitsplätze, regelmäßig getestet?		
Lokation/Benutzer	Gibt es ein Zugriffs- und Berechtigungsverfahren?		

Tabelle 13 (Fortsetzung)

Klassifizierung 1 bis 4 oder Eintrag von Klassifizierungsmerkmalen			
	Bemerkung	Verant-wortlich	
Schnittstellen zu anderen Prozessen und Anwendungen	Inputschnittstellen? Outputschnittstellen? Bereitstellungszeiten? Ergeben sich hieraus Risiken?		
Anwendungs-konzept:	Liegt ein Anwendungskonzept mit den Themen der Nutzung, Verhaltensweise bei Fehlern oder Störungen vor?		
Versicherungen:	Besteht ein besonderes Risiko, das versichert werden muss? Muss eine bestehende Versicherung angepasst werden (Haftpflicht, Betriebsausfallvers.)?		
Bei SLAs:	Vertragspartner Leistungsbeschreibung Hotline, Erreichbarkeit Notfallanweisungen Kontrollstrukturen zur Überwachung		
Ausfallmöglich-keiten und Schwach-stellen:	Welche Ausfälle sind zu betrachten (Notarbeitsplätze, Verlagerung Prozess)? Gibt es Besonderheiten, die zu beachten sind?		
Benötigte Ressourcen:	Geschultes Personal für die Bedienung (User)? Anwendungsbetreuer Berechtigungsmanagement (Adminrechte, Not-User) Changemanagement		
Prüfverfahren:	Test- und Prüfverfahren mit festgelegten Messgrößen.		
Einstufung in die Schutzbedarfsklasse:	Festlegen der Schutzbedarfsklasse: SPA1: kein Schutzbedarf SPA2: geringer Schutzbedarf SPA3: mittlerer Schutzbedarf SPA4: hoher Schutzbedarf		

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

5.2.5 Checkliste Feststellung Schutzbedarfsklassen bei IT-Systemen/IT-Infrastruktur

Durch die Vielschichtigkeit von Präventiv-, Ausfallvermeidungs- und Notfallmaßnahmen kann nur ein Template (siehe Tabelle 14) vorgegeben werden, das entsprechend angepasst und ergänzt werden muss. Diese Checkliste dient einerseits dazu, die Schutzbedarfsklasse und die entsprechenden Anforderungen zu definieren und andererseits erkannte Defizite aufzuzeigen.

Die Schutzbedarfsklasse wird sehr stark geprägt durch Prozesse und Anwendungen, die auf den Systemen und der Infrastruktur laufen. Nicht immer ist für den Systemadministrator erkennbar, welche Prozesse/Anwendungen auf der Infrastruktur und den Systemen laufen und welche Daten übertragen und gespeichert werden. Ebenfalls gibt es technische Dienstleistungen, die in die Geschäftsprozesse schon so

stark eingebunden sind, dass eine Nichtverfügbarkeit enorme Auswirkungen hat (Internet, Intranet, E-Mail). Für die Ermittlung der Schutzbedarfsklasse werden, soweit relevant, die Vertraulichkeit, Verfügbarkeit, Verbindlichkeit und Integrität mit berücksichtigt. Darüber hinaus können weitere Klassifizierungsmerkmale in die rechte Spalte der Tabelle (Tabelle 14) eingetragen werden. In der untersten Zeile kann dann durch die Einzelklassifizierung und durch die Berücksichtigung der zusätzlichen Klassifizierungsmerkmale die Schutzbedarfsklasse SPA festgelegt werden.

Tabelle 14 Checkliste Schutzbedarfsklasse bei Präventiv- und Ausfallvermeidungsmaßnahmen

Klassifizierung 1 bis 4 oder Eintrag von Klassifizierungsmerkmalen			
	Bemerkung	Verant-wortlich	
System:	Name des Systems, Typ		
Bewertung: Verfügbarkeit:	Bewertung: Vertraulichkeit C1 bis C4 Integrität I1 bis I4 Verfügbarkeit A1 bis A4 Verbindlichkeit B1 bis B4 Konkretisierung der notwendigen Verfügbarkeit in Prozent pro Jahr		
Ausfallverträglichkeit:	mögliche zu verkraftende Ausfallzeiten Ausfallzeiten durch Wartung, Changes Wiederbeschaffung, Ersatzbeschaffung Wiederanlaufzeit Verlauf des Schadenpotenzials bei Überschreitung der verträglichen Ausfallzeiten		
Schadenpotenzial:	Welche Risiken sind zusätzlich zu betrachten? (Image-schäden, unmittelbare oder mittelbare Folgeschäden)		
Risiken:	Welche Risiken sind zusätzlich zu betrachten? (Image-schäden, unmittelbare oder mittelbare Folgeschäden, Haftungen)		
Lokation/ Benutzer:	Wer ist Administrator sowie Stellvertreter? Greift das Berechtigungskonzept?		
Anwendungen, die auf dem System laufen:	Name, Kurzbeschreibung, Anwendungsbetreuer Teil eines wichtigen Prozesses, einer Anwendung?		
Betriebskonzept:	Liegt ein Betriebskonzept mit den Themen Datensicherung/Recovery, Wiederanlauf, IT-Security vor?		
Versicherungen:	Besteht ein besonderes Risiko, das versichert werden muss? Muss eine bestehende Versicherung angepasst werden?		
Bei SLAs:	Vertragspartner Leistungsbeschreibung Hotline, Erreichbarkeit Notfallanweisungen Kontrollstrukturen zur Überwachung		
Ausfallmöglichkeiten und Schwachstellen:	Welche Ausfälle sind zu betrachten? Gibt es Besonderheiten, die zu beachten sind?		

Tabelle 14 (Fortsetzung)

Klassifizierung 1 bis 4 oder Eintrag von Klassifizierungsmerkmalen			
	Bemerkung	Verant-wortlich	
Technische Möglich-keiten zur Ausfall-vermeidung:	Welche der Präventiv- und Ausfallvermeidungsmaßnah-men sind angemessen, betriebswirtschaftlich vertretbar und auch vorgesehen? Spiegelung n+1-Technik …		
Benötigte Ressourcen:	Personalressourcen für Wartung, Überprüfung Hardware, Ersatzteile, Wiederbeschaffung Software, Master-CD Zugriffsberechtigung (Adminrechte, Not-User) Kosten		
Zeit-, Umsetzungs-plan:	Installation, Implementierung Schulung, Einweisung Überführung in die Produktion		
Prüfverfahren:	Prüfkonzept mit Festlegung von Messgrößen. Bei gleichartigen Systemen sind Pläne für Stellvertreter-tests vorzugeben Darstellung der Risiken aus der Überprüfung		
Einstufung in Schutz-bedarfsklasse:	Festlegen der Schutzbedarfsklasse SO: kein Schutzbedarf S1: geringer Schutzbedarf S2: mittlerer Schutzbedarf S3: hoher Schutzbedarf		

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

5.2.6 Ermittlung des Gesamtschutzbedarfs

Zur Ermittlung des Gesamtschutzbedarfs „S“ dient die folgende Tabelle (siehe Tabelle 15). Es wird nun mit den festgelegten Schutzbedarfswerten SPA und SIT in der Tabelle die übereinstimmende Spalte gesucht. Nun kann der Schutzbedarf aus der entsprechenden Spalte abgelesen werden.

Tabelle 15 Ermittlung Gesamtschutzbedarf

SPA	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
SIT	1	1	1	1	2	2	2	2	3	3	3	3	4	4	4	4
Schutzbedarf:	S1	S2	S3	S4	S2	S2	S3	S4	S3	S3	S3	S4	S4	S4	S4	S4

Anmerkung: Wenn wenig Informationen vorliegen, so kann bei der Festlegung des Gesamt-schutzbedarfs auch direkt die Klassifizierung vorgegeben werden, ohne dass über die zwei obi-gen Checklisten gegangen wird.

5.2.7 Feststellung der Grundsicherheit von IT-Komponenten und Infrastruktur

Unter Grundsicherheit sind die Maßnahmen zu verstehen, die als Präventiv- und Ausfallvermeidungs- und auch als Notfall- und Kontinuitätsmaßnahmen unabhängig von dem zu betrachtenden Prozess oder von der Anwendung bestehen oder vorgehalten werden (Ist-Zustand). Hierzu zählen USV (unterbrecherfreie Stromversorgung) und Notstromversorgung (Notstromdiesel), Sicherheitseinrichtungen der Technikräume, standardmäßige Datensicherungsmaßnahmen, Backup-RZ, Doppelung von IT-Komponenten und weitere allgemeine Sicherungsmaßnahmen. Eigentlich sind für alle Kern-Geschäftsprozesse und Anwendungen solche Vorkehrungen eingerichtet und bilden eine erhebliche Grundsicherheit. In Notsituationen greifen diese Maßnahmen oft automatisch und der Anwender merkt die Störungs- oder Notsituation nicht.

Für die Feststellung der Grundsicherheit ist der dem Text folgende Smart-Scan (siehe Tabelle 16) anzuwenden. Für die Grundsicherheit ist folgende Kategorisierung vorzunehmen:

- G1 = gering;
- G2 = niedrig;
- G3 = mittel;
- G4 = hoch.

Auf der rechten Seite der folgenden Tabelle gibt es für jede Kategorie eine Spalte mit entsprechend vorbesetzten „Xen“, die auf Basis der einzelnen Fragen und zur Differenzierung der Kategorien gering, niedrig, mittel, hoch unterschiedlich vorgegeben sind. Die Grundsicherheit einer Kategorie ist dann vorhanden, wenn alle vorgesehenen „X“ innerhalb einer Spalte erfüllt sind. Die Tabelle kann natürlich ergänzt und individuell auf die jeweiligen Bedürfnisse des Unternehmens ergänzt und angepasst werden.

Beim Ausfüllen der Tabelle sind die nicht zutreffenden Fragen als erstes zu streichen bzw. es können auch weitere Fragen und Punkte in die Checkliste mit aufgenommen werden. Danach sind die einzelnen Fragen zu beantworten, indem die jeweils zutreffenden Antworten durch ein Kreuz in der vorgesehenen leeren rechten Spalte gekennzeichnet werden. Danach ist eine Übereinstimmung mit der angestrebten Grundsicherheit zu überprüfen, indem die vorgegebene Spalte der Grundsicherheit (hoch, mittel, niedrig, gering) mit der angekreuzten Spalte abgeglichen wird. In den Fällen, wo keine Deckung vorhanden ist, ist die Notwendig von Maßnahmen zur Erlangung der angestrebten Grundsicherheit zu prüfen und durch ein Kreuz in der äußerst rechten Spalte zu kennzeichnen. Bei der Ermittlung des Ergebnisses kann schon der Erfüllungsgrad der angestrebten Grundsicherheit festgestellt werden, indem unter der Tabelle die Anzahl der deckungsgleichen Kreuze in das Ergebnis eingetragen wird. Bei den gekennzeichneten Punkten mit „nicht ausreichenden Maßnahmen“ sind Vorschläge zur Erhöhung der Grundsicherheit vorzugeben.

Tabelle 16 Smart-Scan Grundsicherheit IT-System/Anwendung

Smart-Scan: Feststellung der Grundsicherheit eines IT-Systems, auf dem eine Anwendung läuft							
Maßnahmen nicht ausreichend = × (in Spalte ankreuzen)							↴
G1 = Grundsicherheit gering							
G2 = Grundsicherheit niedrig							
G3 = Grundsicherheit mittel							
G4 = Grundsicherheit hoch							
Ist-Zustand, Zutreffendes in Spalte ankreuzen = ×		↴					
Name der Anwendung: Name, Standort des Systems:	Bemerkung:						
Ist das IT-System an eine USV angeschlossen?	Wie lange hält die USV und welche Auswirkung danach?		×	×	×		
Ist das IT-System an eine Notstromversorgung angeschlossen?	Werden Dieseltests durchgeführt?		×	×			
Steht das IT-System in einem gesicherten Technikraum oder im Rechenzentrum?	Raumüberwachung bzgl. Zugang, Einbruch, Klimatisierung; Sicherheitseinrichtungen gegen Feuer, Wasser;		×	×	×	×	
Ist das IT-System gegen technischen Ausfall durch ein Backup-System gesichert?			×				
Steht das Backup-System in einem anderen Gebäudeteil (Brandabschnitt)?			×				
Gibt es Sicherungseinrichtungen des IT-Systems zur Ausfallvermeidung (Plattenspiegelung, n+1-Technik)?				×			
Gibt es regelmäßige Datensicherungen für das System?	Datenbestand vom Vortag? Werden die Datensicherungen an verschiedenen Orten verwahrt?		×	×	×	×	
Gibt es Recovery-Verfahren? (Fragen können entfallen, wenn für die Anwendungen separate Datensicherungen durchgeführt werden)	Wird das Recovery getestet?		×	×	×	×	

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

Tabelle 16 (Fortsetzung)

Smart-Scan: Feststellung der Grundsicherheit eines IT-Systems, auf dem eine Anwendung läuft							
Maßnahmen nicht ausreichend = × (in Spalte ankreuzen)							↘
G1 = Grundsicherheit gering							
G2 = Grundsicherheit niedrig							
G3 = Grundsicherheit mittel							
G4 = Grundsicherheit hoch							
Ist-Zustand, Zutreffendes in Spalte ankreuzen = × ↘							
Sind Verantwortliche für die Betreuung des IT-Systems vorhanden und bekannt?	Verfügbarkeit der Systemverantwortlichen während und außerhalb der Arbeitszeit? Gibt es Stellvertreterregelungen?		×	×	×	×	
Gibt es SLAs, wenn Leistungen durch Dienstleister erbracht werden (Rechenzentrum)?	Sind die zu erbringenden Leistungen klar umschrieben und bekannt?		×	×	×	×	
Gibt es Wartungsverträge (für Hardware, Systemsoftware, Wiederbeschaffung, Hotline, etc.)?	Welche Leistungen werden abgedeckt, welche Antwortzeiten und Wiederbeschaffungszeiten sind vorgesehen?		×	×	×	×	
Wird dieses System in Notfallübungen mit einbezogen?	Wurden Notfall-, K-Fall-Übungen durchgeführt?		×	×			
Ist die IT-Infrastruktur (LAN, WAN) ebenfalls ausfallsicher ausgelegt?	Netzwerk gedoppelt, USV und Notstrom, …?		×	×			
Ergebnis (Summe):			12	11	7	6	

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

5.2.8 Feststellung der Sicherheit und Verfügbarkeit von Anwendungen

Über die Grundsicherheit hinaus bestehen bei den Prozessen/Anwendungen zusätzliche Notfall- und Kontinuitätskonzepte, soweit diese betriebswirtschaftlich vertretbar sind. Hiermit werden nicht nur die gesetzlichen Auflagen (KonTraG, GoB, …) erfüllt, sondern auch aus Eigeninteresse des Unternehmens in Not- oder Krisenfällen eine Aufrechterhaltung und Steuerung der Geschäftstätigkeit in einem vertretbaren Maße gewährleistet. Anhand der vorgegebenen Klassifizierung in der folgenden Tabelle (siehe Tabelle 17) kann die Klassifizierung der Risikovorsorge (V1–V4) anhand des Ist-Zustands ermittelt werden.

Tabelle 17 Smart-Scan-Einschätzung Risikovorsorge

Smart-Scan: Einschätzung der Risikovorsorge (Sicherheit/Verfügbarkeit) einer Anwendung							
Maßnahmen nicht ausreichend = × (in Spalte ankreuzen)							↓
V1 = Sicherheit/Verfügbarkeit gering							
V2 = Sicherheit/Verfügbarkeit niedrig							
V3 = Sicherheit/Verfügbarkeit mittel							
V4 = Sicherheit/Verfügbarkeit hoch							
Ist-Zustand, Zutreffendes in Spalte ankreuzen = ×		↓					
Name der Anwendung:	Bemerkung:						
Steht die Anwendung in dem geforderten Maß zur Verfügung?	Anforderung der Verfügbarkeit des FB gegenüber der tatsächlichen Verfügbarkeit prüfen (Accounting)		×	×	×	×	
Ist die Anwendung fehlertolerant oder hochverfügbar programmiert?			×				
Gibt es einen Test- und Changeprozess bei Neuinstallation, bei Programmänderungen und bei Releases- oder Versionswechsel?	Wird die Anwendung auf ihre gesamtheitliche Funktion und auf Performance geprüft? – Black-, Whiteboxtest – Funktionstest – Integrationstest – Regressionstest		×	×	×		
Gibt es einen Notfall- und Kontinuitätsplan, der im K-Fall den Ablauf regelt?			×	×	×		
Wird der Notfallplan, die Notfallorganisation regelmäßig getestet?	Gibt es hierzu bisherige Verfahren, Testdokumente und Protokolle?		×	×			
Sind Zugriffsrechte geregelt?	Kann ein Benutzer nur die ihm zugeordneten Daten lesen, anlegen, ändern und löschen? Gibt es ein Logging und wird dieses kontrolliert?		×	×	×	×	
Sind Maßnahmen zur Verhinderung der Manipulation (auch Ausspähung) von Daten und Programmen installiert? (Hackerangriffe, Sabotage, Spionage)	Firewall, PKI, Verschlüsselung, physische Trennung, …?		×	×			
Sind Verantwortliche für die Betreuung der Anwendung vorhanden?	Zu welchen Zeiten stehen Betreuer zur Verfügung? Gibt es mindestens einen Stellvertreter?		×	×	×		
Gibt es regelmäßige Datensicherungen für diese Anwendung?	Datenbestand vom Vortag? Werden die Datensicherungen an verschiedenen Orten verwahrt?		×	×	×	×	

Tabelle 17 (Fortsetzung)

Smart-Scan: Einschätzung der Risikovorsorge (Sicherheit/Verfügbarkeit) einer Anwendung							
Maßnahmen nicht ausreichend = × (in Spalte ankreuzen)							
V1 = Sicherheit/Verfügbarkeit gering							
V2 = Sicherheit/Verfügbarkeit niedrig							
V3 = Sicherheit/Verfügbarkeit mittel							
V4 = Sicherheit/Verfügbarkeit hoch							
Ist-Zustand, Zutreffendes in Spalte ankreuzen = ×							
Gibt es ein Recovery- und Wiederanlaufverfahren? Gibt es eine Nacherfassung von Daten?	Wird Recovery- und Wiederanlauf getestet? Wird die Datenintegrität nach einem Wiederanlauf geprüft?		×	×	×		
Gibt es ein Betriebskonzept?			×	×	×		
Ergebnis:			11	10	8	3	

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

5.2.9 Feststellung der Risikovorsorge

Die beiden Smart-Scan-Tabellen beinhalten Überschneidungen von Sicherheitsmaßnahmen. Zur Zusammenführung und Bestimmung der Gesamt-Risikovorsorge werden die Grundsicherheit (G1–G4) und die Risikovorsorge (V1–V4) in der folgende Übersicht (siehe Tabelle 18) zusammengeführt:

Tabelle 18 Grundsicherheit IT-Systeme

Tabelle Risikovorsorge (Sicherheit/Verfügbarkeit) der Anwendung					hoch G4	mittel G3	niedrig G2	gering G1
Gesamt-Risiko-vorsorge	hoch V4	mittel V3	niedrig V2	gering V1				
GV4					×			
GV4		×			×			
GV3	×					×		
GV3		×				×		
GV3			×		×			
GV2		×					×	
GV2			×			×	×	
GV1			×					×
GV1				×	×	×	×	×

5.2.10 Feststellung des Risikos

Zur Feststellung des Risikos wird der Ist-Zustand (Risikovorsorge) dem Soll-Zustand (Schutzbedarf) gegenübergestellt (siehe Tabelle 19).

Tabelle 19 Risikobestimmung aus Vorsorge und Schutzbedarf

	Risikovorsorge			
Schutzbedarf	**GV4**	**GV3**	**GV2**	**GV1**
S4	K1	K2	K3	K4
S3	K1*	K1	K2	K3
S2	K1*	K1*	K1	K2
S1	K1*	K1*	K1*	K1

- K4 = unmittelbarer Handlungsbedarf
- K3 = Handlungsbedarf
- K2 = möglicher Handlungsbedarf, Risiko ist tragbar
- K1 = kein Handlungsbedarf

Anmerkung: K1* = möglicher Handlungsbedarf zur Kosteneinsparung, weil die Gesamt-Risikovorsorge über den Anforderungen des Schutzbedarfs liegt.

Das hier festgestellte Risiko ist anhand folgender Fragestellungen noch anzupassen, wobei eine farbliche Umstufung im Gesamtkontext zu bewerten und entsprechend im Reporting aufzuzeigen ist:

- Ist der Zeitpunkt für eine regelmäßig vorgesehene Notfallübung oder Überprüfung von Präventiv- und Ausfallvermeidungsmaßnahmen erheblich überschritten, so ist das Risiko farblich höher einzustufen. Ist dieser Zeitpunkt um mehr als ein Jahr überschritten, so ist das Risiko farblich um eine weitere Stufe zu erhöhen.
- Weiterhin ist die Aktualität der Dokumente, SLAs und insbesondere die Zuständigkeit bei den Schutzbedarfsklassen S3 und S4 sicherzustellen (Überprüfung einmal pro Jahr). Bei Unvollständigkeit und fehlender Aktualität kann hier das Risiko ebenfalls farblich höher eingestuft werden.

5.2.11 Zuordnung und Bewertung der Risikoanalyse für die FMEA

Für die Kurzanalyse der FMEA ist nun ein grober Funktionsbaum zu erstellen, wobei auf der obersten Ebene (Level 1) die Anwendung steht. Auf der darunter liegenden Ebene (Level 2) wird nach Möglichkeit die Struktur Eingabe, Verarbeitung und Ausgabe (EVA-Prinzip) vorgesehen. Auf der dritten Ebene (Level 3) sind die wichtigsten und fehleranfälligsten Funktionen und Vorgänge anzuordnen.

Methodisch wird nun jeder weitere Schritt der FMEA bearbeitet, wobei als nächstes der Fehlerbaum erstellt, eine Gewichtung und Priorisierung der Fehlfunktionen durchgeführt sowie die Bewertung der Fehlfunktionen vorgenommen wird.

In die Bewertung fließen die bisherigen Erkenntnisse aus der Risikoanalyse ein. Entsprechende zusätzliche Erkenntnisse aus der FMEA sind in einer Auf- oder Abstufung der Bewertung mit zu berücksichtigen.

5.2.12 Überführung der Bewertung in die FMEA

Festlegung der Bedeutung „B“ anhand der Wichtigkeit, wobei für die Prozesse/ Anwendungen die Schutzbedarfsklasse benutzt wird (siehe Tabelle 20):

Tabelle 20 Zuordnung „B“

Schutzbedarfsklasse	Bedeutung „B“	
S1	1–2	gering
S2	3–5	niedrig
S3	6–7	mittel
S4	8–9	hoch
S4	10	Gesetzliche Anforderungen

Festlegen der Auftrittswahrscheinlichkeit „A“ anhand der Ergebnisse aus der Risikoanalyse und der festgestellten Risikovorsorge mit folgender Tabelle (siehe Tabelle 21):

Tabelle 21 Zuordnung „A“

Risikovorsorge	Auftretenswahrscheinlichkeit „A“	
GV1	8–10	Grundsicherheit gering
GV2	6–7	Grundsicherheit niedrig
GV3	3–5	Grundsicherheit mittel
GV4	1–2	Grundsicherheit hoch

Festlegung der Entdeckungswahrscheinlichkeit „E“, wobei anhand der ermittelten Risikovorsorge folgende Zuordnung getroffen wird (siehe Tabelle22):

Tabelle 22 Zuordnung „E“

Gesamt-Risikovorsorge	Entdeckungswahrscheinlichkeit „E“
GV1	5–10
GV2	3–4
GV3	2
GV4	1

Nachdem für alle Prozesse/Anwendungen eine Risikoanalyse und Risikoeinschätzung durchgeführt wurde, ist methodisch durch eine Expertenklausur eine Gesamteinschätzung des Prozesses vorzunehmen.

Kapitel 6
Das IT-Security & Contingency Management

6.1 Warum IT-Security & Contingency Management?

Um Produkte und Dienstleistungen in der erforderlichen Art und Weise den Kunden anbieten zu können, ist der reibungslose Ablauf von Geschäftsprozessen erforderlich. Für den Ablauf eines Geschäftsprozesses wiederum ist das Zusammenspiel von Informations- und Kommunikationstechnik, Mensch und Infrastruktur notwendig.

Da Störungen von Geschäftsprozessen niemals ausgeschlossen werden können, ist sicherzustellen, dass das Schadenpotenzial bei Störungen der wichtigen Prozesse steuerbar ist, so dass Geschäfte auch dann noch in einem vertretbaren Rahmen getätigt werden können. Hierunter ist zu verstehen, dass bei Störungen der wichtigen Prozesse der Geschäftsbetrieb unter betriebswirtschaftlich und unternehmerisch vertretbaren Aspekten kontrolliert und steuerbar aufrechterhalten oder aber bewusst eingestellt wird, um das Schadenspotenzial für das Unternehmen zu minimieren.

Um dieses Ziel der Schadensminimierung bzw. -vermeidung nach Möglichkeit zu erreichen und somit eigenen Anforderungen sowie gesetzlichen Vorgaben zu genügen, ist die Einrichtung eines IT-Security & Contingency Managements eine wichtige Position in einem Unternehmen, die implizit auch die Funktion des Security-Officers wahrnimmt.

An dieser Stelle bleibt anzumerken, dass das IT-Security & Contingency Management nicht Risiken berücksichtigt, die sich aus der mangelnden Verfügbarkeit von Mensch (Mitarbeiter) und Infrastruktur (Haustechnik, etc.) ergeben. Für die Verfügbarkeit der Mitarbeiter in Notfällen haben die entsprechenden Bereiche bzw. Abteilungen Sorge zu tragen. Für infrastrukturelle Notfälle z. B. durch mangelnde Verfügbarkeit der Gebäudetechnik (Strom-, Wasser-, Klimaausfall, etc.) ist die Gebäude- und Hausverwaltung zuständig und deren Notfallkonzepte maßgebend; diese Konzepte sind aber, insoweit aufbau- und ablauforganisatorische, beim IT-Security & Contingency Management mit in die eigenen Konzepte, Verfahren und Abläufe mit einzubeziehen. Primäre Aufgabenstellung des IT-Security

K. H. W. Thies, *Management operationaler IT- und Prozess-Risiken,*

© Springer 2008

& Contingency Management sind die Erstellung, Aktualisierung, Schulung, Einweisung und auch die Überwachung der Einhaltung von IT-Sicherheits-, Präventiv-, Ausfall- und Kontinuitätskonzepten.

6.2 Risiken im Fokus des IT-Security & Contingency Managements

Jedes Unternehmen ist bei der Wahrnehmung seines ureigenen Geschäfts verschiedenen Risiken ausgesetzt. Risiken werden zum Teil bewusst zur Wahrung von Geschäftschancen in Kauf genommen. Risiko, d. h. die negative Abweichung von dem Erwartungswert und somit die Gefahr unerwarteter Verluste, und Rendite stehen hierbei in einem engen Zusammenhang. Zu diesen Risiken gehören Marktpreisrisiko, Ausfallrisiko, Liquiditätsrisiko, strategisches Risiko und auch operationales Risiko.

Das operationale Risiko kann weiter in Personal-, Geschäftsprozess-, Rechts-, Katastrophen-, Reputations- und Technologierisiko untergliedert werden.

Gefahren, die in den Bereichen der Hardware, DV-Infrastruktur sowie der System- und Anwendungssoftware und der darauf ablaufenden Geschäftsprozesse bestehen, werden allgemein als operationales IT-Risiko zusammengefasst. Dieses Risiko ist primär im Fokus des IT-Security & Contingency Managements.

6.3 Aufbau und Ablauforganisation des IT-Security & Contingency Managements

6.3.1 Zuständigkeiten

Das IT-Security & Contingency Management mit seiner Richtlinienkompetenz verantwortet folgende Themen:

- Unternehmenspolicies, Richtlinien, Anweisungen zu IT-Sicherheits-Themen;
- Vorgaben für IT-Sicherheitsanforderungen und -maßnahmen;
- Notfall- und Kontinuitätskonzepte;
- Notfall-, K-Fall-Übungen;
- IT-Risikomanagement;
- Support in K-Fall-Situationen.

Inhaltlich sind diese Themen bestimmt durch die Zuständigkeit für die Evaluierung und Umsetzung von IT-Sicherheitsanforderungen, Vorgabe von Methoden, Tools und Verfahren zu IT-Sicherheits- und Kontinuitätsthemen sowie zu leistende Beratung der Fachbereiche, Kompetenzcenter, Anwendungs- und Systembetreuer bei der Erarbeitung, Umsetzung und Überprüfung von Präventiv-, Notfall- und Kontinuitätsmaßnahmen.

Darüber hinaus führt das IT-Security & Contingency Management die notwendigen Informationen des operationalen IT-Risikos für eine IT-Risikosteuerung zusammen.

In K-Fall-Situationen werden der operationale und strategische Krisenstab sowie die tangierten Fachbereiche und Kompetenzcenter unterstützt und koordiniert.

6.3.2 Aufbauorganisation

Von der Aufbauorganisation her sind folgende Themen zu besetzen (siehe Abb. 23):

- Teamleitung und Funktion Security-Officer;
- Contingency Management für die Geschäftsprozesse/Anwendungen;
- Security & Prevention für den IT-Systembetrieb (Produktion);
- IT-Risk Controlling.

Als ein wichtiger Erfolgsgarant ist das IT-Security & Contingency Management aufbauorganisatorisch auf einer möglichst hohen hierarchischen Ebene anzusiedeln, um direkte Eskalationswege zur Geschäftsführung zu ermöglichen. So kann das IT-Security & Contingency Management z. B. in der ersten Ebene des

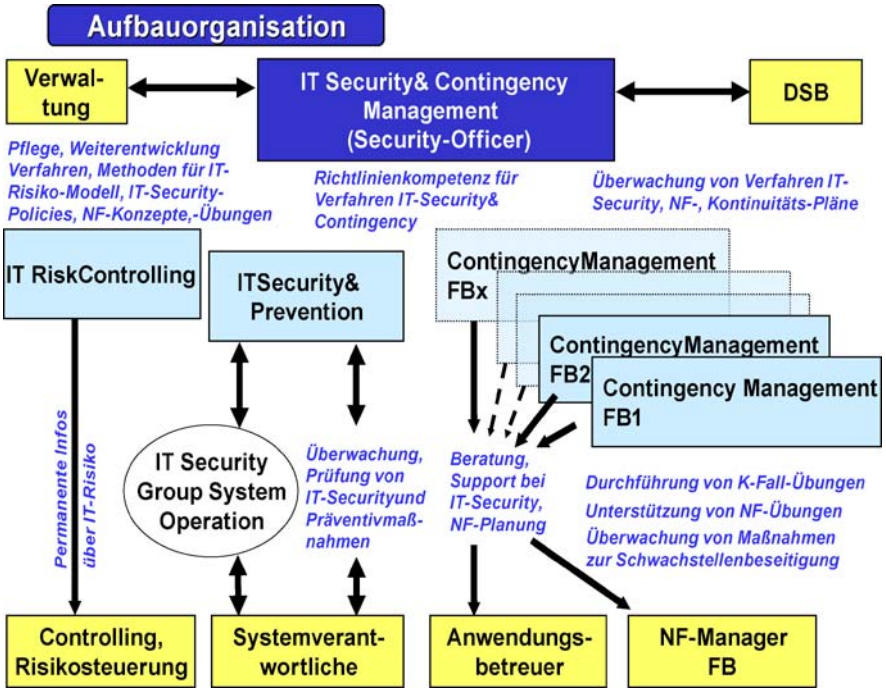


Abb. 23 Aufbauorganisation des IT-Security & Contingency Managements

Bereichs Betriebsorganisation/Informatik, Risk-Management, Controlling untergebracht oder auch direkt der Geschäftsführung zugeordnet werden.

6.3.3 Teamleitung IT-Security & Contingency Management

Dem Teamleiter, der auch die Funktion Security-Officer mit abdeckt, obliegt die Koordination innerhalb des IT-Security & Contingency Managements. Er delegiert Aufgaben, führt Ergebnisse zusammen und kommuniziert diese an das Risk-Controlling bzw. an die Unternehmenssteuerung und an die ihm disziplinarisch übergeordnete Ebene. Er ist auch für eine zentrale Bereitstellung einer Notfall-DB zuständig, indem alle Präventiv-, Notfall- und Kontinuitätsmaßnahmen sowie die Überprüfungsprotokolle eingestellt und bei Wechsel historisiert werden können.

6.3.4 Rolle: Security & Prevention IT-Systeme/Infrastruktur

Die Rolle IT-Systeme/Infrastruktur als Teil des IT-Security & Contingency Managements:

- entwickelt grundsätzliche und übergreifende Vorgaben zum Thema Informationssicherheit;
- passt bestehende IT-Security-Policies an und entwickelt sie weiter;
- initiiert und überwacht die Umsetzung spezifischer Sicherheitsmaßnahmen;
- überwacht die regelmäßige Überprüfung von Präventivmaßnahmen im Umfeld der IT-Systeme und IT-Infrastruktur;
- Koordiniert die IT-Security Group System Operation (Arbeitskreis IT-Sicherheit).

6.3.5 Rolle: Contingency Management Fachbereichsbetreuung

Das Contingency Management ist für die Fachbereichsbetreuung zuständig. Seine Aufgaben sind:

- Vorgabe von Methoden, Tools, Verfahrensanweisungen;
- Beratung und Unterstützung bei der Durchführung von Risiko- und Schwachstellenanalyse;
- Unterstützung bei der Erstellung von Präventiv-, NF- und Kontinuitätsplänen;
- Beratung und Unterstützung bei der Planung und Durchführung von NF-Übungen;
- Überwachung dringlicher Maßnahmenumsetzungen.

6.3.6 Rolle: IT-Risikosteuerung

Die IT-Risikosteuerung ist für folgende Aufgaben verantwortlich:

- regelmäßige Bewertung des operationalen IT-Risikos, d. h. die Zusammenführung der Daten aus den Einzelbewertungen der IT-Risiken auf Produkt-/Prozessebene (z. B. aus FMEAs);
- Ansprechpartner und Schnittstelle zum Risk-Management, bzw. zum Unternehmenscontrolling;
- entwickelt und passt das IT-Risikomodell an neue Anforderungen an.

6.3.7 Schnittstellen zu anderen Bereichen

Systemverantwortlicher

Der Systemverantwortliche:

- überprüft die Notwendigkeit einzelner bestehender technischer Präventivmaßnahmen;
- überprüft die Notwendigkeit neuer Präventivmaßnahmen und setzt diese um;
- überprüft die Funktionsfähigkeit von technischen Präventivmaßnahmen;
- überprüft die ihn betreffenden NF- und Kontinuitätspläne auf ihren Inhalt und gleicht sie ggf. an;
- ist fester Teilnehmer der IT-Security-Group-System-Operation.

Anwendungsbetreuer

Der Anwendungsbetreuer:

- überprüft die Notwendigkeit einzelner bestehender technischer Präventivmaßnahmen in Zusammenarbeit mit den Verantwortlichen im Fachbereich;
- überprüft die Notwendigkeit für neue Präventivmaßnahmen und initiiert ggf. deren Erstellung in Abstimmung mit dem zuständigen Fachbereich;
- überprüft die Funktionsfähigkeit von technischen Präventivmaßnahmen;
- überprüft die NF-Pläne auf ihren Inhalt und gleicht sie ggf. für die zu betreuende Anwendung in Abstimmung mit dem tangierten Fachbereich an;
- wirkt bei der Durchführung von NF- und K-Fall-Übungen mit.

Notfallmanager Fachbereich

In jedem Fachbereich, mindestens aber auf der Bereichsebene, ist ein Notfallmanager (Stabsstelle) sowie ein Stellvertreter zu benennen. Hierfür bieten sich

mögliche vorhandene DV- oder IT-Koordinatoren an, die in vielen Fällen mit der Thematik schon vertraut sind.

Allgemeine Aufgaben:

- direkter Ansprechpartner für das IT-Security & Contingency Management;
- Reporting an das IT-Security & Contingency Management;
- Überprüfung der Existenz von Betriebskonzepten und notwendigen SLAs für alle wichtigen produktiven Anwendungen und Systeme im zugehörigen FB; gilt auch bei größeren Changes oder der Einführung neuer Anwendungen und Systeme;
- unterstützende Tätigkeit beim IT-Risikomanagement.

Aufgaben in Bezug auf NF-Pläne:

- Überprüfung der Notwendigkeit von NF- und Kontinuitätsplänen;
- regelmäßige Überprüfung der NF- und Kontinuitätspläne auf deren inhaltliche Richtigkeit und Vollständigkeit bei Neueinführung von Anwendungen, IT-Systemen, bei komplexeren Prozessänderungen und auch bei Personal- oder Zuständigkeitswechsel (Umorganisation);
- Anweisung zur Aktualisierung von NF-und Kontinuitätsplänen;
- Verteilung der NF- und Kontinuitätspläne an die tangierten Mitarbeiter im FB, an den Anwendungsbetreuer KC und an das IT-Security & Contingency Management;
- Vorhalten der NF- und Kontinuitätspläne im FB an einem für die betroffenen Mitarbeiter im Not- oder K-Fall leicht zugänglichen Ort;
- Sicherstellen, dass die Mitarbeiter mit den NF- und Kontinuitätsplänen hinreichend vertraut sind (Einweisung, Schulung, Übungen).

In Bezug auf Präventivmaßnahmen:

- Überprüfung der Notwendigkeit und inhaltlichen Richtigkeit von Präventivmaßnahmen;
- Regelmäßige Überprüfung der Umsetzung von Präventivmaßnahmen;
- Vorhalten notwendiger Unterlagen und Hilfsmittel an einem für die tangierten Mitarbeiter im Notfall leicht zugänglichen Ort;
- Sicherstellen, dass die Mitarbeiter mit den Präventivmaßnahmen hinreichend vertraut sind (Einweisung, Schulung);
- Bei technischen Präventivmaßnahmen ist eine regelmäßige Überprüfung der Funktion zu gewährleisten und nachzuweisen.

Im Bezug auf die IT-Security Group System Operation:

- bei Bedarf Teilnahme an den Sitzungen der IT-Security Group System Operation.

Notfall-/K-Fall-Übungen:

- Unterstützung bei der Planung von NF-/K-Fall-Übungen im FB;
- Koordination von NF-/K-Fall-Übungen im FB;
- Nachbereitung von NF-/K-Fall-Übungen.

In Notfall- und K-Fall-Situationen:

- beruft den operativen Krisenstab ein;
- koordiniert alle Notfallaktivitäten im FB mit entsprechender Weisungsbefugnis aus Aufträgen des operativen Krisenstabs;
- stellt Statusberichte zusammen und berichtet direkt an den operativen Krisenstab;
- erstellt Vorschläge für Problemlösungen und weiteres Vorgehen;
- dokumentiert und wertet die Notfall-/K-Fall-Situation aus;
- initiiert und kontrolliert die Beseitigung von Schwachstellen im Rahmen der Nachbearbeitung.

Jeder neu erstellte Notfall- und Kontinuitätsplan wird bei der Produktionsübergabe vom zuständigen Notfallmanager in eine Notfall-DB eingestellt. Ebenfalls wird jeder aktualisierte Notfall- und Kontinuitätsplan im Rahmen des Changeprozesses mit eingepflegt, wobei der vorhergehende Plan historisiert wird.

Betriebs- und Gebäudeverwaltung (Facility-Management)

Immer wenn es Berührungspunkte zwischen Präventivmaßnahmen, Störungen, Notfällen, K-Fällen gibt, die in Zusammenhang mit der Haus- und Gebäudesicherheit stehen, ist das entsprechende Team der Verwaltung zu informieren und in Entscheidungsabläufe des IT-Security & Contingency Managements einzubinden.

DSB (Datenschutzbeauftragter)

Der Datenschutzbeauftragte ist bzgl. aller Maßnahmen des IT-Security & Contingency Managements, die in engem Zusammenhang mit persönlichen, vertraulichen Daten stehen und für die Umsetzung des Datenschutzgesetzes (BDSG) relevant sind oder sein könnten, zu informieren bzw. in Entscheidungsabläufe einzubinden. Die Einbindung des DSB bezieht sich insbesondere auf Präventivmaßnahmen und Maßnahmen des IT-Security & Contingency Managements, die außerhalb von Notfall- und K-Fall-Situationen getroffen werden.

Während tatsächlicher Notfall- und K-Fall-Situationen ist die Einhaltung des Datenschutzes zu gewährleisten, soweit dies situativ zumutbar und betriebswirtschaftlich vertretbar ist.

Betriebsrat

Der Betriebsrat ist bzgl. aller Maßnahmen des IT-Security & Contingency Managements, die nach dem Betriebsverfassungsgesetz mitbestimmungspflichtig sind, mit einzubeziehen. Dies gilt im Zusammenhang mit persönlichen Daten, aber auch mit Bereitschafts-, Verfügbarkeitsregelungen sowie örtlichem Wechsel in

Notarbeitsplätze bei Notfall- bzw. K-Fall-Übungen. Es ist eine Regelung empfehlenswert, wie während tätsachlich eingetretener Notfall- und K-Fall-Situationen mit Themen, die mitbestimmungspflichtig sind, umgegangen wird. In diesen Fällen sollten die Regelungen und Betriebsvereinbarungen eingehalten werden und der Betriebsrat zeitnah informiert werden, soweit dies situativ zumutbar und betriebswirtschaftlich vertretbar ist.

Unternehmenssteuerung, Risk-Controlling

Die Unternehmensrisikosteuerung bzw. das Risk-Controlling wird regelmäßig von der IT-Risikosteuerung des IT-Security & Contingency Managements über Ergebnisse der IT-Schwachstellenanalyse und Risikoeinschätzung informiert. In Zusammenarbeit zwischen dem IT-Security & Contingency Management und der Unternehmenssteuerung bzw. dem Risk-Controlling werden Konzepte entwickelt und folgend aktualisiert, die die IT-Risikoeinschätzung im Rahmen der Unternehmens-Risikoeinschätzung berücksichtigen und ggf. Einfluss auf das Rating des eigenen Unternehmens haben.

6.3.8 Besondere Aufgaben

Notfall-DB

Das IT-Security & Contingency Management stellt eine Notfall-DB bereit, in die alle Präventiv-, Notfall- und Kontinuitätsmaßnahmen sowie Überprüfungsprotokolle und Testunterlagen eingestellt und bei Changes entsprechend historisiert werden.

Arbeitskreis IT-Security Group System Operation

Die IT-Security Group System Operation tritt viermal im Jahr, jeweils zum ersten Donnerstag, der ein Werktag ist, an einem vorgegebenen Ort zusammen, falls nicht ein anderer Zyklus vereinbart wurde. Verantwortlich für die Koordination und Durchführung ist der Mitarbeiter des IT-Security & Contingency Managements, der für das Thema IT-Security & Prävention IT zuständig ist. Der Arbeitskreis befasst sich mit der Planung, Realisierung, dem Betreiben und der Überwachung von IT-System-Sicherheit, stimmt Aktivitäten ab und legt Standards fest. Insbesondere beschäftigt er sich auch mit aufgetretenen Sicherheitsverletzungen und Notsituationen und leitet Maßnahmen zur Beseitigung erkannter Schwachstellen ein. Im Rahmen von Beschlussfassungen kann der Arbeitskreis Aufträge vorgeben, die vom IT-Security & Contingency Management zur Entscheidung gebracht und umgesetzt werden.

Die IT-Security Group System Operation setzt sich wie folgt zusammen:

Tabelle 23 Arbeitskreis Security Group System Operation

Feste Teilnehmer:	Bedarfsweise Teilnehmer:
IT Security & Prevention IT	DSB
Betreuung Internet/Notes/Outlook	Rechtsbereich
Betreuung Netzwerk	Revision
Betreuung Server, PCs	FB
Providermanagement	Anwendungsbetreuer
Berechtigungsverwaltung	Rechenzentrum
Changemanagement/Testcenter	Telekommunikationsanbieter
…	Betriebsrat

Durchführung von K-Fall-Übungen

Zur Überprüfung des komplexen Zusammenspiels mehrerer Notfall- und Kontinuitätspläne und Sicherungsmaßnahmen ist mindestens einmal jährlich vom IT-Security & Contingency Management eine K-Fall-Übung durchzuführen. Hierzu gehören Planung, Durchführung und Auswertung, wobei die tangierten FB, System- und Anwendungsbetreuer unmittelbar in diese K-Fall-Übung mit einbezogen werden. Im Vorfeld ist durch Vorstandsbeschluss die K-Fall-Übung zu genehmigen.

6.3.9 Anforderungsprofil an Mitarbeiter des IT-Security & Contingency Managements

Anforderungsprofil für die Teamleitung

Anzahl: ein Mitarbeiter

Zuständig für die Themen:

- Fachliche und disziplinarische Teamführung;
- IT-Security (konzeptionell und methodisch);
- Ausfallvermeidungsmaßnahmen (konzeptionell und methodisch);
- Notfallmaßnahmen und -übungen (konzeptionell und methodisch);
- Initiierung von K-Fall-Übungen;
- Einschätzung von operationalen IT-Risiken;
- Unterstützung der Krisenstäbe;
- Dokumentation von Methoden, Verfahren, Policies und Richtlinien;
- Notfall-DB.

Aufgabenstellung:

- Koordination sowie fachliche und disziplinarische Führung des Teams;
- Initiierung und Controlling der Maßnahmenumsetzung zur Minderung von Risiken aus erkannten Schwachstellen;
- Controlling der regelmäßigen Prüfungen von Sicherheitsmaßnahmen und Notfallübungen;
- Erstellung regelmäßiger Statusberichte;
- Mitglied im operativen Krisenstab für Koordination und Moderation.

DV-Kenntnisse/System-Kenntnisse:

- Kenntnisse über die bestehende Systemlandschaft des Unternehmens;
- Grundkenntnisse über IT-Security (Viren, Firewall, Contentscanning, PKI, …) sowie über Berechtigungs- und Zugriffsverfahren;
- Allgemeinkenntnisse über Vermeidungsmaßnahmen technischer Ausfälle, fehlertolerante Systeme, Datensicherungs- und Recovery-Verfahren.

Organisatorische/methodische Kenntnisse:

- Projekterfahrung, Krisenmanagement;
- Organisations- und Managementerfahrung;
- Personalführungserfahrung;
- Allgemeines methodisches Basiswissen;
- Präsentations- und Moderationserfahrung.

Fachliche Kenntnisse:

- Grundkenntnisse betriebswirtschaftlicher Zusammenhänge des Unternehmens.

Zusätzliche Kenntnisse und Fähigkeiten:

- Teamfähig;
- belastbar und konfliktfähig;
- durchsetzungsfähig.

Anforderungsprofil für Mitarbeiter (IT-Security & Prevention)

Anzahl: je nach Unternehmensgröße mindestens ein Mitarbeiter, der dieses Thema verantwortet.

Zuständig für die Themen:

- Technische Infrastruktur, WLAN/LAN/WAN;
- C/S;
- Host;
- Intra-, Internet-Security.

Aufgabenstellung:

- Zugangsberechtigung, Zugriffsschutz, Firewall, Verschlüsselungsverfahren, …;
- Schwachstellenanalyse, Maßnahmen der Beseitigung, Risikoeinschätzung;
- Verfolgung der Maßnahmenumsetzung zur Minderung von Risiken aus erkannten Schwachstellen;
- Überwachung, dass regelmäßige Prüfungen von Sicherheitsmaßnahmen durchgeführt werden;
- Beratung über Möglichkeiten von Sicherheitsmaßnahmen zur Vermeidung von Ausfällen, deren Umsetzungsmöglichkeiten und Festlegung von Prüfkriterien;
- Permanente Beobachtung der Changeprozesse und Feststellung möglicher Auswirkungen auf das IT-Risiko;
- Leitung und Steuerung des Arbeitskreises IT-Security Group System Operation;
- Ansprechpartner NF- und K-Fall-Übungen gegenüber Dienstleistern;
- Zusammenstellung und Aktualisierung von Risikodaten für die technische Infrastruktur.

DV-Kenntnisse/System-Kenntnisse:

- Detaillierte Kenntnisse über die bestehende Systemlandschaft des Unternehmens;
- Detaillierte Kenntnisse über technische Schutzmaßnahmen, wie Viren- bzw. Contentscanning, Firewall, Verschlüsselungen, etc.;
- Maßnahmen zur Vermeidung technischer Ausfälle, fehlertolerante Systeme;
- Datensicherungs- und Recovery-Verfahren.

Organisatorische/methodische Kenntnisse:

- Projekterfahrung, Krisenmanagement;
- Selbstorganisation;
- Methodisches Basiswissen (Kosten-/Nutzen-Analyse, Entscheidungstabellen, Schwachstellen-Analyse, Terminplanung und -verfolgung, etc.);
- Präsentations- und Moderationserfahrung.

Unternehmensbezogene, betriebswirtschaftliche Kenntnisse:

- Kenntnisse der unternehmensbetrieblichen Zusammenhänge (wünschenswert).

Wünschenswerte zusätzliche Kenntnisse und Fähigkeiten:

- Teamfähig;
- belastbar und konfliktfähig;
- durchsetzungsfähig;
- Notfall-, K-Fall-Kenntnisse oder -Erfahrungen.

Anforderungsprofil für Mitarbeiter mit Schwerpunkt Notfall- und Kontinuitätsmanagement in den einzelnen Fachbereichen

Anzahl: für jeden wichtigen Fachbereich sollte ein Mitarbeiter vorgesehen werden.

Zuständig für die Themen des jeweils zu betreuenden Fachbereichs:

- Risikobetrachtung der Prozesse und Anwendungen;
- Präventiv-, Notfall- und Kontinuitätsmaßnahmen;
- Notfall-, K-Fall-Übungen;
- Schulung, Sensibilisierung.

Aufgabenstellung:

- Schwachstellenanalyse und Risikoeinschätzung der jeweiligen Prozesse und Anwendungen, Überprüfung der Notfallpläne;
- Verfolgung der Maßnahmenumsetzung zur Minderung von Risiken aus erkannten Schwachstellen der Anwendungen, Prozesse und NF-Pläne;
- Risikoeinschätzung der Anwendungen und Prozesse;
- Unterstützung des Notfallmanagers bei der Initiierung, Planung und Durchführung von NF-Übungen;
- Beratung über Möglichkeiten von Sicherheitsmaßnahmen zur Vermeidung oder Milderung von Ausfällen;
- Beratung und Unterstützung bei NF-Plänen und bei Planung von NF-Übungen inkl. Festlegung von Prüfkriterien;
- Permanente Beobachtung der Changeprozesse und Feststellung möglicher Auswirkungen auf das IT-Risiko der Prozesse im entsprechenden Fach-bereich;
- Zusammenstellung und Aktualisierung von Risikodaten für den entsprechenden Fachbereich;
- Mitwirkung bei der Initiierung, Planung und Durchführung von K-Fall-Übungen.

DV-Kenntnisse/System-Kenntnisse:

- Überblick über die bestehende Systemlandschaft des Unternehmens;
- Grundkenntnisse über Maßnahmen zur Vermeidung technischer Ausfälle, fehlertolerante Systeme, Datensicherungs- und Recovery-Verfahren.

Organisatorische, methodische Kenntnisse:

- Projekterfahrung, Krisenmanagement;
- Selbstorganisation;
- methodisches Basiswissen (Kosten-/Nutzen-Analyse, Entscheidungstabellen, Schwachstellen-Analyse (z. B. FMEA), Terminplanung und -verfolgung, etc.);
- Präsentations- und Moderationserfahrung.

Fachliche, betriebswirtschaftliche Kenntnisse:

- Umfassende Kenntnisse der im Fachbereich eingesetzten Anwendungen und ablaufenden Prozesse.

Wünschenswerte zusätzliche Kenntnisse und Fähigkeiten:

- Teamfähig;
- belastbar und konfliktfähig;
- durchsetzungsfähig;
- Notfall-, K-Fall-Kenntnisse oder -Erfahrungen.

Mitarbeiterprofil für IT-Risikosteuerung, Methoden & Tools

Anzahl: abhängig von der Unternehmensgröße, mindestens aber ein Mitarbeiter, der dieses Thema primär verantwortet.

Zuständig für die Themen:

- Methoden und Verfahren;
- Dokumentation;
- IT-Risikocontrolling;
- Reporting IT-Risiken;
- Aufbau- und Ablauforganisation Krisenmanagement.

Aufgabenstellung:

- Pflege und Weiterentwicklung des Modells IT-Risikocontrolling;
- Meldung der IT-Risikoeinschätzung an Risk-Controlling bzw. an die Unternehmenssteuerung;
- Pflege und Weiterentwicklung der Methoden und Tools, Konzepte, Verfahren;
- Aufbau und Funktion des operationalen und strategischen Krisenmanagements;
- Dokumentation und Pflege der Dokumentation;
- Unterstützung bei der Schwachstellen-Analyse;
- Support bei Anwendung von Methoden und Tools;
- Zusammenfassung der IT-Risikodaten für das Reporting.

DV-Kenntnisse/System-Kenntnisse:

- Überblick über die bestehende Systemlandschaft des Unternehmens;
- Grundkenntnisse über technische Schutzmaßnahmen, wie Viren-, Contentscanning, Firewall, Verschlüsselungen, …;
- Grundkenntnisse über Maßnahmen zur Vermeidung technischer Ausfälle, fehlertolerante Systeme, Datensicherungs- und Recovery-Verfahren.

Organisatorische, methodische Kenntnisse:

- Projekterfahrung, Krisenmanagement;
- Selbstorganisation;
- umfassendes methodisches Wissen;
- Präsentations- und Moderationserfahrung.

Fachliche, betriebswirtschaftliche Kenntnisse:

- Kenntnisse über die Zusammenhänge der Prozesse und Anwendungen.

Wünschenswerte zusätzliche Kenntnisse und Fähigkeiten:

- teamfähig;
- belastbar und konfliktfähig;
- Notfall-, K-Fall-Kenntnisse oder -Erfahrungen.

Kapitel 7
IT-Krisenorganisation

7.1 Aufbauorganisation des IT-Krisenmanagements

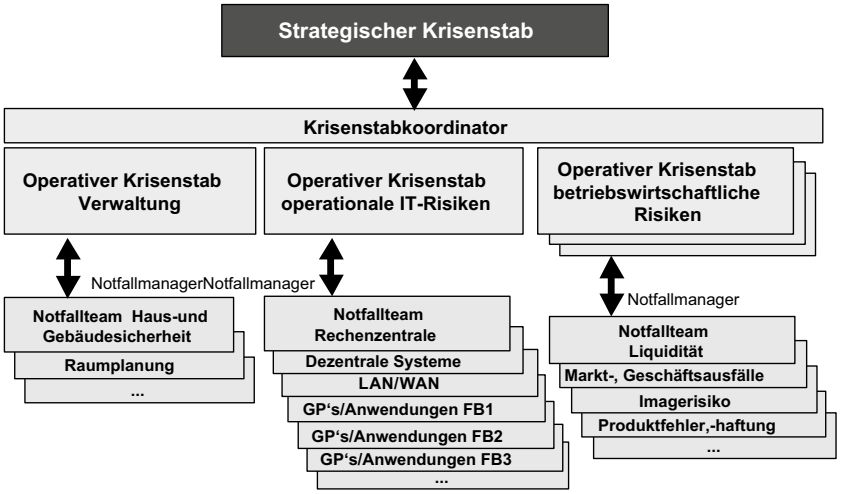


Abb. 24 Aufbau einer Krisenorganisation

7.2 Zusammensetzung, Kompetenzen und Informationspflichten der Krisenstäbe

Im Nachfolgenden wird der Aufbau einer Krisenorganisation dargestellt (siehe Abb. 24).

© Springer 2008

7.2.1 Operativer Krisenstab

Zusammensetzung

- Bereichsleiter oder Stellvertreter der tangierten Fachbereiche;
- Weitere unmittelbar tangierte Führungskräfte aus der zweiten Führungsebene;
- Security-Officer bzw. Teamleiter IT-Security & Contingency Management als Moderator und in beratender Funktion;
- Datenschutzbeauftragter;
- Betriebsrat.

Kompetenzen

- Feststellung und Erklärung des Not- bzw. K-Falls;
- Bestätigen, dass Notfall- und Kontinuitätspläne in Kraft treten, bzw. in Kraft bleiben;
- Durch Beschluss wird der strategische Krisenstab einberufen;
- Aufzeigen von Lösungen zur Bewältigung der Krise gegenüber dem strategischen Krisenstab;
- Zweckgebundener Budgetrahmen zur Schadensbegrenzung, für Reparatur und Wiederbeschaffung je Krisenfall;
- Für die Umsetzung von gefassten Beschlüssen besteht volle Weisungsbefugnis;
- Übergeordnete Leitung und Koordination aller Aktivitäten;
- Einleitung von Maßnahmen zur Fehlerlokalisierung, -behebung und zum Wiederanlauf;
- Deklaration des Endes des Notfalls.

Informationspflichten

- Zusammenstellung von Informationen und Entscheidungshilfen für den strategischen Krisenstab:
  - Statusberichte;
  - Schadensbericht;
  - Zeitplan, Prognosen zur Schadensbehebung und zum Wiederanlauf;
  - Entscheidungsvorlagen;
  - Empfehlungen für Öffentlichkeitsarbeit;
  - Bereichsleiter informiert immer direkt die zuständigen Geschäftsführer, Vorstand;
- Abteilungsleiter initiiert, informiert und koordiniert alle Maßnahmen in seiner Abteilung;
- Teamleiter IT-Security & Contingency Management informiert seine eigene Gruppe.

7.2.2 Strategischer Krisenstab

Zusammensetzung

- Geschäftsführung, Vorstand stellt immer den Leiter und Sprecher des Krisenstabs;
- optional können weitere Führungskräfte in den Krisenstab einberufen werden;
- Bereichsleiter Öffentlichkeitsarbeit, Pressesprecher;
- optional Bereichsleiter Personal;
- optional Bereichsleiter Rechtsfragen;
- optional weitere Bereichsleiter tangierter Fachbereiche;
- etc.

Kompetenzen

- K-Fall bestätigen;
- weisungsbefugt gegenüber dem operativen Krisenstab;
- Herbeiführung von Entscheidungen und Freigabe von Budget;
- Steuerung der Öffentlichkeitsarbeit;
- Ende des K-Falls bestätigen.

Informationspflichten

- Berichtet über Art, Ausmaß, Verlauf des Schadens und Problembehebung gegenüber dem Aufsichtsrat und Aufsichtsbehörden;
- Öffentlichkeitsarbeit in das Unternehmen hinein und nach außen.

7.3 Verhältnis zwischen den beiden Krisenstäben

Der operative Krisenstab ist das Bindeglied zwischen dem strategischen Krisenstab und den Fachbereichen, den Serviceeinheiten, den Dienstleistern und Kunden. Er bereitet Status-Informationen und Entscheidungsvorlagen für den strategischen Krisenstab vor und setzt dessen Anweisungen und Beschlüsse um (siehe Abb. 24).

7.4 Zusammenkunft des Krisenstabs (Kommandozentrale)

Der operationale Krisenstab trifft sich normalerweise immer in der Kommandozentrale. Wenn diese nicht verfügbar ist, so ist der Treffpunkt der Ausweichraum

1, ist dieser ebenfalls nicht verfügbar, so ist der Treffpunkt der Ausweichraum 2. Zur klaren Festlegung kann die folgende Tabelle genutzt werden:

Tabelle 24 Festlegung Kommandozentrale

Kommandozentrale	Ausweichraum 1	Ausweichraum 2
Gebäude: Raum: Tel.	Gebäude: Raum: Tel.	Gebäude: Raum: Tel.

In der Kommandozentrale ist folgende Ausrüstung vorzuhalten:

- ausreichende Möblierung (Tische, Stühle, Schreibtische, etc.);
- zwei interne Hausanschlüsse im eigenen Telefonnetz sowie Fax-Anschluss;
- zwei Postanschlüsse;
- mindestens ein betriebsbereites Handy, bei mehreren Handys sind unterschiedliche Netzbetreiber vorzusehen; Handys sind entsprechend soweit mit den jeweiligen Adress- und Telefon-Nr. konfiguriert;
- aktuelles internes Telefonverzeichnis;
- zwei PCs, besser Notebooks mit Netzwerkanschluss (LAN oder WLAN), die entsprechend konfiguriert und mit Software sowie aktuellen Daten (Telefonverzeichnis, Adressen, Notfallpläne, …) versehen sind; hierzu auch jeweils ausreichende Ersatzakkus;
- alle Notfallpläne in lesbarer Form;
- Flipchart, 2 Metaplanwände, Schreib- und Moderationsmaterial.

Der operative Krisenstab sorgt für einen Raum, in dem sich der strategische Krisenstab treffen und tagen kann.

Im Notfall sind von den Mitgliedern der Krisenstäbe mitzubringen:

- betriebsbereites Handy, incl. Ladegerät;
- Schreibutensilien;
- aktuelle Notfallpläne;
- Telefon und Handylisten der Mitarbeiter;
- eigenes Notebook mit Netzteil;
- weitere wichtig erscheinende Unterlagen und Hilfsmittel.

7.5 Auslöser für die Aktivierung des Krisenstabs

Der Verlauf eines Notfalls bzw. K-Falls verläuft eigentlich immer nach dem gleichen Muster. Es tritt ein Ereignis ein, das zu Störungen von Prozessen oder Anwendungen führt. Nach der ersten Sondierung der Ursache ist möglicherweise schon erkennbar, ob diese Störung mit den normalen organisatorischen Mitteln zu bewältigen ist oder ob ein möglicher Notfall oder K-Fall besteht bzw. sich entwickeln kann. Nach Ablauf gewisser vorgegebener Reaktionszeiten wird der operative

Krisenstab einberufen. Nach Sachlage und Dringlichkeit alarmiert der operative Krisenstab dann den strategischen Krisenstab. In vielen Fällen unterscheiden sich die Not-Situationen durch eine unterschiedliche Zeitspanne und Reaktionszeit, wobei bei sehr kurzen Zeiten Aktionen sogar zusammenfallen können. In der nachfolgenden Tabelle werden die einzelnen Szenarien und ihre Auswirkungen im Kontext dargestellt.

Tabelle 25 Übersicht der Notfall-, K-Fall-Phasen

	Störung:	Notfall:	K-Fall:
Ereignis:	Die Funktionalität einer Anwendung ist beeinträchtigt, aber noch funktionsfähig, oder eine Anwendung fällt kurzzeitig aus, angefallene Arbeit kann unproblematisch nachgearbeitet werden.	Ausfall einer Anwendung, eines Prozesses auf unbestimmte Zeit; Möglichkeit eines hohen monetären Schadens ist absehbar.	Gravierender Ausfall oder Nichtverfügbarkeit von Anwendungen, Prozessen, Gebäuden, die aufgrund ihres Zusammenwirkens zu einem unternehmensgefährdenden Schaden führen können.
Reaktion, verantwortliche Person:	1) unmittelbare Weitergabe der Störungsmeldung an den User Help Desk, der informiert Anwendungs-, Systembetreuung; 2) Unverzüglich Vorgesetzten informieren, Anweisungen abwarten; Statusinfo an die Mitarbeiter, bei denen die Störung eingetreten ist.	1) Meldung wie bei Störung; 2) Wird kritische Ausfallzeit (siehe NF- u. Kontinuitätsplan) überschritten, dann Inkraftsetzung des NF- u. Kontinuitätsplans; Info an die disziplinarischen Vorgesetzten; 3) Einberufung des operativen Krisenstabs durch den disziplinarischen Vorgesetzten; 4) Mitarbeiter über Status und weiteres Vorgehen informieren.	1) Meldung wie bei Störung; 2) Wird kritische Ausfallzeit überschritten, dann Inkraftsetzen des NF- u. Kontinuitätsplans; Vorgesetzte unverzüglich informieren; 2) Einberufung des operativen Krisenstabs durch die disziplinarischen Vorgesetzten; 3) Mitarbeiter über Status und weiteres Vorgehen informieren; 4) Einberufung des strategischen Krisenstabs durch den operativen Krisenstab.

Im folgenden Beispiel (siehe Tabelle 26) sind die einzelnen Notfall- und Krisen-Phasen im Überblick schematisch dargestellt. Die aufgeführten Reaktionszeiten sind als Maximalfristen zu sehen und sollten nach Möglichkeit nicht überschritten werden. Für alle wichtigen Prozesse sind solche Tabellen mit den Reaktionszeiten und Aktivitäten festzulegen. Die Reaktionszeiten können möglicherweise von Prozess zu Prozess sehr unterschiedlich sein, sie dienen aber zur Steuerung von Abläufen in Not- und Krisensituationen, ebenso die Aktivitäten in den einzelnen Phasen. Den einzelnen Phasen sind dann auch die Krisenstufen Defcon 5 bis Defcon 1 zugeordnet, wobei Defcon 5 die Stufe beschreibt, in der keine Störung, kein Not- oder K-Fall vorliegt (Friedenszeit).

Tabelle 26 Übersicht über Reaktionszeiten

Reaktions-zeit	Beschreibung der Phase	Krisen-stufen
	Produktion läuft ohne Störungen und Fehler	Defcon 5
	Mit Auftreten einer Störung greifen Präventivmaßnahmen, die die Störung umgehen, wie z. B. Systeme gedoppelt; der Benutzer bekommt hiervon in den seltensten Fällen etwas mit. System-, Anwendungsbetreuung lokalisiert und behebt den Fehler im laufenden Betrieb.	Defcon 4
sofort	Mit der Kenntnisnahme der Störung bzw. des Notfalls durch den Benutzer ist der UHD unverzüglich zu verständigen; UHD informiert Systembetreuer, Anwendungsbetreuer oder Dienstleister zwecks Fehlerlokalisierung, -behebung.	
bis zu 1 Std.	Einberufung des operativen Krisenstabs; Aktivieren der Notfall- und Kontinuitätspläne, wobei dies in vielen Fällen eine Einschränkung des Geschäftsbetriebs bedeutet.	Defcon 3
bis zu 2 Std.	Entscheidung, ob Notfall vorliegt; Aufnahme der Arbeit durch den operativen Krisenstab. Erklärung des Not-, bzw. K-Falls.	Defcon 2
bis zu 3 Std.	operativer Krisenstab teilt Notfall und weitere Vorgehensweise den tangierten Mitarbeitern mit; Einberufung weiterer Kompetenz-/Know-how-Träger in den operativen Krisenstab; Bildung von Arbeitsgruppen zur Krisenbewältigung; Einleitung von Sofortmaßnahmen.	
bis zu 6 Std.	Erstellung eines Maßnahmenkatalogs zur Notfallbewältigung vom operativen Krisenstab; Einberufung des strategischen Krisenstabs; Statusbericht und Entscheidungsvorlagen an den strategischen Krisenstab.	Defcon 1
bis zu 12 Std.	Sofortmaßnahmen sind alle eingeleitet; Maßnahmen zur Bewältigung der Notsituation sind initiiert; Öffentlichkeitsarbeit, Presseberichte durch den strategischen Krisenstab.	
bis zu 24 Std.	Notbetrieb ist produktiv, Frontoffice arbeitet ohne große Einschränkungen.	Defcon 2
bis zu 48 Std.	Backoffice arbeitet im Notbetrieb.	
bis zu 60 Std.	Einleitung aller notwendigen Maßnahmen zur Erreichung des normalen Geschäftsbetriebs sind initiiert (Wiederanlauf).	Defcon 3
bis zu 120 Std.	Nacherfassung von Geschäftsvorgängen ist zum Großteil abgeschlossen; Datenintegrität ist hergestellt; Überleitung in den normalen Geschäftsbetrieb.	Defcon 4
danach	operativer Krisenstab • übergibt Koordination an entsprechenden OEen; • teilt das Ende des Not-, K-Falls mit; • analysiert, dokumentiert die Notfallmaßnahmen; • erklärt die Arbeit des Krisenstabs für beendet; • IT-Security & Contingency Management und FB/KC werten den Notfall, K-Fall aus; • leiten Maßnahmen zur Schwachstellenbeseitigung ein; • überprüfen die IT-Risikoeinschätzung.	Defcon 5

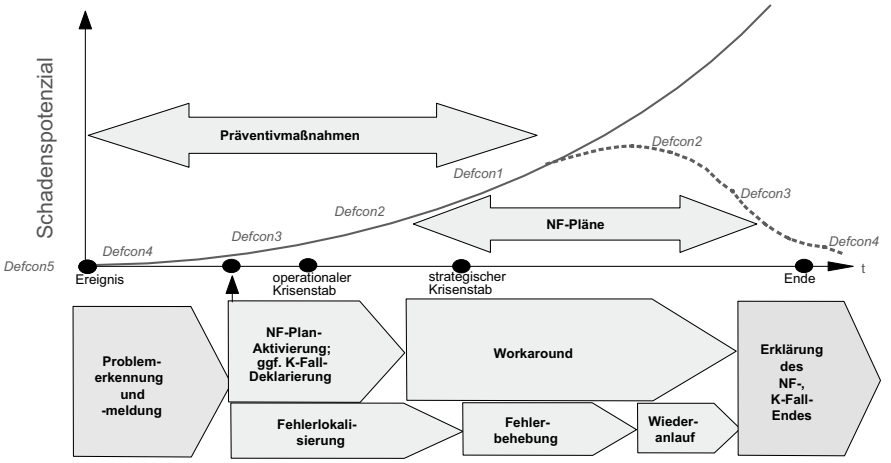


Abb. 25 Ereignis-/Schadendiagramm

Ebenfalls ist der Schadenverlauf für jeden wichtigen Prozess zu ermitteln und festzulegen (siehe Abb. 25). Anhand des Kurvenverlaufes sind sehr einfach die notwendigen Reaktionszeiten abzuleiten.

Wenn das Ereignis innerhalb der Rahmenarbeitszeit aufgetreten ist, beginnt die Reaktionszeit sofort; außerhalb der Rahmenarbeitszeit beginnt die Reaktionszeit mit der Inkraftsetzung der Notfall- und Kontinuitätspläne und Einberufung des operativen Krisenstabs, spätestens aber zu Beginn der Rahmenarbeitszeit des nächsten Arbeitstages. Die Arbeitszeit kann z. B. wie folgt festgelegt sein:

Rahmenarbeitszeit:	7:00 Uhr–18:00 Uhr
Kernarbeitszeit:	8:45 Uhr–16:00 Uhr

Werden vorgegebene Reaktionszeiten überschritten, so wird seitens des operativen Krisenstabs die Eskalation zum strategischen Krisenstab bzw. zu Geschäftsführung oder Vorstand eingeleitet.

7.6 Arbeitsaufnahme des operativen Krisenstabs

Nach der Einberufung des operativen Krisenstabs tritt dieser in der Kommandozentrale zu einem bekannt gegebenen Zeitpunkt zusammen. Als erstes wird der Leiter und Sprecher des operativen Krisenstabs festgelegt. Dann wird die Sachlage sondiert und ein Lagebericht erstellt. Im Folgenden wird entschieden, ob ein Notfall oder K-Fall vorliegt und ob der operative Krisenstab seine Arbeit aufnimmt.

Ist eine Notfallsituation nicht eindeutig identifizierbar, so ist der operative Krisenstab zwecks Handlungsfähigkeit ermächtigt und auch verpflichtet, schnellstmöglich Klärung über den Sachverhalt herbeizuführen.

Liegt keine Notfallsituation vor, so löst sich der operative Krisenstab unmittelbar auf und der Sachverhalt wird der Geschäftsführung bzw. dem Vorstand zeitnah berichtet.

Liegt ein Notfall vor, so entscheidet der operative Krisenstab, ob der strategische Krisenstab einberufen wird. Danach stehen beide Krisenstäbe in ständiger Verbindung, stimmen sich ab, führen Beschlüsse herbei, leiten Maßnahmen ein und überwachen und steuern die Umsetzung und den Fortschritt zur Bewältigung der Notsituation.

Folgende Notfallmaßnahmen müssen selbständig vom operativen Krisenstab initiiert und durchgeführt werden:

- Mitteilung an die betroffenen Mitarbeiter über das Vorliegen einer Notfallsituation;
- Benennen und Einberufen weiterer Kompetenz- und Know-how-Träger in den operativen Krisenstab;
- Festlegen der Informations- und Kommunikationswege (Telefon, FAX, E-Mail, etc.);
- Bildung von Arbeitsgruppen mit Aufgabenzuteilungen;
- Festlegen der Teilnehmer und der Termine für Krisenstabssitzungen;
- Einleitung erster Maßnahmen zur Schadensbegrenzung;
- Umsetzung der Notfallpläne zur Gewährleistung eines Notbetriebs;
- Festlegen eines Maßnahmenkatalogs zur Bewältigung der Notsituation;
- Überführung des Notbetriebes in den normalen Geschäftsbetrieb;
- Erarbeitung eines Erfahrungsberichtes mit Schwachstellenanalyse;
- Auflösung des operativen Krisenstabs.

7.6.1 Bilden von Arbeitsgruppen

Der operative Krisenstab stellt die notwendigen Maßnahmen fest, bildet Arbeitskreise und delegiert die Maßnahmen zur Umsetzung an die entsprechenden Arbeitkreise (siehe Abb. 26). Für jeden Arbeitskreis sind ein Sprecher und ein Stellvertreter zu benennen. Bei Fremdfirmen und Dienstleistern müssen wegen der kurzen Wege Koordinatoren eingesetzt werden. Die Arbeitsgruppen sind situationsbezogen zu bilden, wobei nachstehende Gruppen wie folgt definiert sind:

- **Fachbereich 1 bis n** (jeweils pro FB ein Zuständiger/Stellvertreter)
  - Verantwortlich für Prozesse/Anwendungen und Umsetzung der Notfall- und Kontinuitätspläne;
  - Verantwortlich für Bestandsaufnahme und regelmäßige Feststellung des Schadenverlaufs der zu verantwortenden Prozesse;
  - Umzug in Notarbeitsplätze sowie Arbeitsaufnahme;
  - Mitwirkung beim Wiederanlauf.

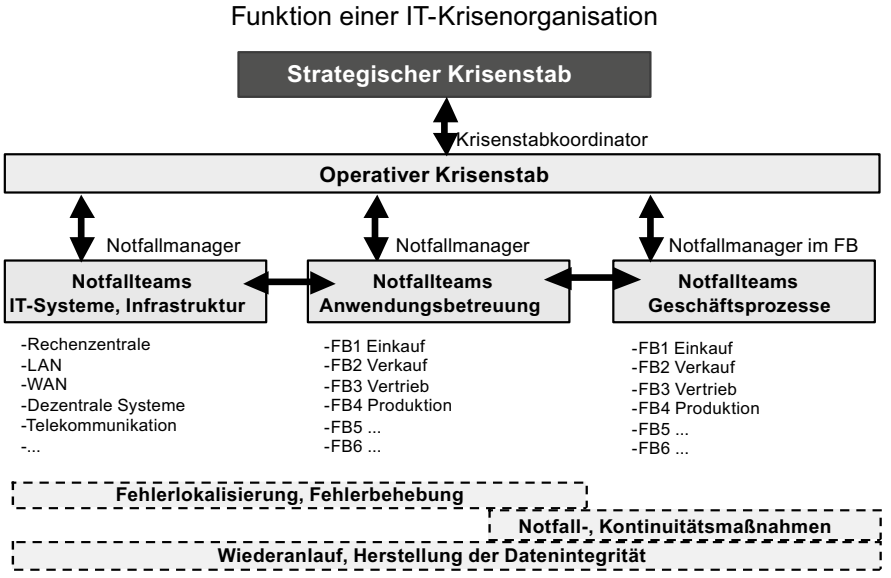


Abb. 26 Organigramm Krisenstäbe

- **Haustechnik/Infrastruktur**
  - Verantwortlich für Bestandsaufnahme;
  - Erarbeiten von Alternativen für Strom-, Wasser-, Klimaversorgung und Haustechnik.
- **Raumplanung**
  - Verantwortlich für Bestandsaufnahme bei Flächenausfall;
  - Bereitstellung von Flächen und Büromöbeln als Interimslösung.
- **Verwaltung**
  - Bereitstellung von Sicherheitspersonal.
- **Beschaffung/Einkauf**
  - Bereitstellung, Wiederbeschaffung von Hardware, PCs.
- **Netzwerke LAN/IT-Infrastruktur**
  - Verantwortlich für die Wiederherstellung der LAN- und WLAN-Infrastruktur und der Schnittstellen zum WAN.
- **Host/Rechenzentralen, dezentrale Systeme, IT-Infrastruktur** (Koordinator zum RZ)
  - Verantwortlicher Koordinator für die Bereitstellung von Hostanwendungen und konsistenten Datenbeständen in Zusammenarbeit mit den Rechenzentralen;
  - Verantwortlich für die Wiederherstellung der dezentralen Systeme und Server.

- **Telekommunikation, WAN** (Koordinator zum Telekomdienstleister)
  - Verantwortlich für Telefonanlage;
  - Verantwortlich für WAN-Anbindungen.

7.6.2 Unterlagen für den Krisenstab

Aktivitäten-Checkliste für den Koordinator des operativen Krisenstabs

Die folgende Checkliste (siehe Tabelle 27) dient dem Krisenkoordinator als Vorlage für die Initiierung und Überwachung notwendiger Aktivitäten. Die Aufgabe übernimmt der Teamleiter IT-Security & Contingency Management.

Tabelle 27 Aktivitäten-Checkliste für den Koordinator

Phase	Aktivitäten	erledigt
Aufbieten des operativen Krisenstabs	Mitglieder des operativen Krisenstabs kontaktieren, informieren und beordern (Ort, Raum, Datum, Zeit)	
	Sitzungsraum aufsuchen	
	Zutritt zu Gebäude und Sitzungsraum offen halten	
	Unterlagen und Hilfsmittel bereitlegen	
Sitzung des operativen Krisenstabs	Festlegen des Leiters/Sprechers und der Stellvertretung des Krisenstabs (Rollen und Kompetenzen festlegen)	
	Veranlassung der Schadensfeststellung und mögliche Auswirkungen aufzeigen (Berichte von den aktiven Notfallmanagern)	
	Statusbericht mit abgeschlossenen, laufenden und initiierten Maßnahmen, Risikoeinschätzung und Schadenverlauf erstellen	
	Feststellung der Notfallsituation (Beschluss) Bekanntgabe, Ausruf der Notsituation Festlegen, wann und unter welchen Umständen der strategische Krisenstab informiert und einberufen werden soll	
	Notfall- und Kontinuitätspläne in Kraft setzen (feststellen welche!)	
	Einberufen von Arbeitsgruppen (Sprecher festgelegt) • Fachbereich 1 • Fachbereich 2 • Fachbereich n • Haustechnik/Infrastruktur • Raumplanung (Flächen, Möbel) • Verwaltung/Sicherheitsdienst • LAN-Management • Dezentrale Systeme, Server • Dienstleister • Host/Rechenzentrum • Telekommunikation, WAN	

Tabelle 27 (Fortsetzung)

Phase	Aktivitäten	erledigt
Sitzung des operativen Krisenstabs	Delegieren von Aktivitäten an Arbeitsgruppen mit Zieldefinitionen, Checkpoints und Terminvorgaben	
	Aktivierung des strategischen Krisenstabs • Beschluss zur Einberufung des strategischen Krisenstabs • Teilnehmer festlegen • Einberufung mit Angabe Ort, Raum, Datum und Uhrzeit • Statusbericht, Entscheidungsvorlagen, Öffentlichkeitsarbeit	
Organisatorische Maßnahmen	Telefon in der Kommandozentrale besetzen	
	Aufbau der Kommunikationsstruktur und -wege, damit Mitglieder des jeweiligen Krisenstabs kontaktiert, informiert und beordert werden können	
	• Arbeitsplätze bereitstellen (Notarbeitsplätze), • Unwichtige Abteilungen ausdünnen und von der Arbeit freistellen	
	• Problem-, To-Do-Liste erstellen, aktualisieren, fortschreiben, • augenblickliche Schadenfeststellung, Schadenverlauf darstellen, • Netzplan mit Abhängigkeiten und Terminen, • Maßnahmenkatalog je Arbeitsgruppe	
	Informationsaustausch der Arbeitsgruppen gewährleistet	
	Zutritt zu Sicherheitsarchiven sicherstellen	
	Unterkunft und Verpflegung organisieren	
	Öffentlichkeitsarbeit	

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

Alarmierungsplan

Gerade in der hektischen Anfangsphase eines Notfalls oder einer Katastrophe ist es wichtig, dass Aufgaben systematisch abgearbeitet und protokolliert werden. Für die Alarmierungsphase folgt ein Template eines Alamierungsplans (siehe Tabelle 28), der im Vorfeld schon mit allen notwenigen Informationen ausgefüllt werden muss:

Tabelle 28 Alarmierungsplan/-checkliste

Funktion	Name/ Stellvertreter	Telefon			Benachrichtigung erledigt
Operativer Krisenstab:		Büro	Handy	Privat	
Leitung Einkauf					
Leitung Produktion 1					
Leitung Produktion 2					
Leitung Vertrieb					
Leitung Finanzen					
Leitung IT/ORG					

Tabelle 28 (Fortsetzung)

Funktion	Name/ Stellvertreter	Telefon			Benachrichtigung erledigt
Bereichsleitung Verwaltung					
IT-Security & Contingency Management					
Datenschutzbeauftragter					
Betriebsrat					
Strategischer Krisenstab:					
Vorsitzender GF					
GF Einkauf					
GF Produktion					
GF Verkauf, Vertrieb					
Leiter Unternehmens-kommunikation					
Leiter Personal					

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

Sitzungsprotokoll des operativen/strategischen Krisenstabs

Nach Eintreffen aller Teilnehmer wird unverzüglich die Sitzung eröffnet und folgendes Protokoll erstellt:

Tabelle 29 Sitzungsprotokoll Krisenstab

	Name	Tel.-Nr.
Leiter/Sprecher Krisenstab	Name des Sprechers (Krisenstabkoordinator)	
Anwesende Teilnehmer	Teilnehmer 1	
	Teilnehmer 2	
	Teilnehmer 3	
	Teilnehmer 4	
	Teilnehmer 5	
Protokollführer	Festlegen des Protokollführers	
Sprecher DV-Krisenstab	Festlegen des Sprechers für Infos, Öffentlichkeitsarbeit	

	Maßnahmen/Aktivitäten
Grobanalyse Lage	Situationsbericht durch den Krisenstabkoordinator:
	• Problembeschreibung, Überblick
	• bisher abgeschlossene Aktivitäten und Abklärungen
	• laufende Aktivitäten und Abklärungen
	• geplante Aktivitäten und Abklärungen

Tabelle 29 (Fortsetzung)

Weiteres Vorgehen	Strukturieren und Festlegen der Vorgehensweise und Aktivitäten
	Festlegung, wann der strategische Krisenstab einberufen und informiert werden soll
	Verteilen der Aufgaben an die Teilnehmer
	Festlegen von Checkpoints und Terminen
	Absprache der Berichts- und Kommunikationswege
	Festlegen der nächsten Krisensitzung
	Erstellung eines Ablaufplans durch den Krisenstabkoordinator
	Erstellung eines Statusberichts für den strategischen Krisenstab
	Information des strategischen Krisenstabs durch den Sprecher des operativen Krisenstabs

Krisenstab-Beschluss

In Notfallsituationen müssen Maßnahmen eingeleitet werden, die die Kompetenzen des Einzelnen überschreiten, bzw. bei denen eine Unsicherheit bzgl. der Entscheidungskompetenz besteht. In diesen und generell bei wichtigen Beschlüssen ist die Beschlussfassung (siehe Tabelle 30) schriftlich zu fixieren. Beschlussfähig ist hier die einfache Mehrheit des operativen Krisenstabs. Falls die Kompetenzen des operativen Krisenstabs überschritten werden, so ist eine Entscheidungsvorlage für den strategischen Krisenstab zu erstellen und die Genehmigung einzuholen.

Tabelle 30 Krisenstab-Beschluss

Beschluss des: • operativen Krisenstabs • strategischen Krisenstabs	Datum:	Uhrzeit:
Text		
Name	Unterschrift	
Name in Blockbuchstaben		

7.7 Verfahrensanweisungen zu einzelnen K-Fall-Situationen

7.7.1 Brand

- Identifikation des Szenarios;
- Einleitung von Sofortmaßnahmen zur Schadensbegrenzung;
- Alarmierungsplan für Sofortmaßnahmen;
  - Feuerwehr, wenn nicht schon automatisch geschehen;
  - Situativ Polizei oder weitere Behörden informieren;
  - Verwaltung;
  - Fachbereiche;
  - IT/ORG, RZ, Dienstleister;
- Alarmierung des operativen Krisenstabs (wer, wann, wo);
- Krisensitzung operativer Krisenstab;
  - Situation erfassen;
  - Schadensausmaß feststellen;
  - Sofortmaßnahmen zur Schadensbegrenzung;
  - Maßnahmen zur Sicherung des Geschäftsbetriebs (Notfallpläne aktivieren);
  - Beschlussfassung/Empfehlung von weiteren Aktivitäten für den strategischen Krisenstab (Entscheidungsvorlagen);
- Alarmierung des strategischen Krisenstabs;
- Krisensitzung strategischer Krisenstab;
  - Bericht über Situation und Schadensausmaß durch operativen Krisenstab;
  - Unterbreitung von Entscheidungsvorlagen durch operativen Krisenstab;
  - Beschlussfassung für Sofortmaßnahmen zur Schadensbegrenzung und zur Unternehmenssicherung;
- Steuerung der Öffentlichkeitsarbeit;
- Umsetzung und Steuerung von Maßnahmen durch den operativen Krisenstab;
  - Koordination der Notfallaktivitäten;
  - Statusmeldungen;
  - Umsetzung von Öffentlichkeitsarbeit;
  - Beschlussfassung und Empfehlung weiterer Maßnahmen;
  - Feststellung des Endes der Notfallsituation;
- Deklaration des Endes der Notfall-, K-Fall-Situation durch den operativen Krisenstab, nach Beschluss durch den Strategischen Krisenstab.

7.7.2 Wassereinbruch

Ablauf wie bei Brand (Nichtzutreffendes aus der Liste entfällt, Notwendiges ist entsprechend mit einzufügen).

7.7.3 Stromausfall

Ablauf wie bei Brand (Nichtzutreffendes aus der Liste entfällt, Notwendiges ist entsprechend mit einzufügen).

7.7.4 Ausfall der Klimaanlage

Ablauf wie bei Brand (Nichtzutreffendes aus der Liste entfällt, Notwendiges ist entsprechend mit einzufügen).

7.7.5 Flugzeugabsturz

Ablauf wie bei Brand (Nichtzutreffendes aus der Liste entfällt, Notwendiges ist entsprechend mit einzufügen).

7.7.6 Geiselnahme

Ablauf muss individuell vorgegeben werden. Grundsätzlich kann hier ebenfalls die Verfahrensweise wie bei Brand genommen werden, wobei der Schwerpunkt nun eher auf der polizeilichen Seite zu sehen ist. Bei Geiselnahme ist zu beachten, dass oftmals das gesamte Gebäude geräumt wird und großräumig das Areal abgesperrt wird!

7.7.7 Ausfall der Datenübertragung intern, zum RZ, zu den Kunden

Bei gravierenden Störungen der Kommunikationsverbindungen, die zu einer Krisensituation führen, ist wie folgt zu verfahren:

- Identifikation des Szenarios;
- Einleitung von Sofortmaßnahmen zur Schadensbegrenzung;
- Alarmierungsplan für Sofortmaßnahmen;
  - Fachbereiche;
  - IT/ORG, RZ, Dienstleister;

- Alarmierung des operativen Krisenstabs (Wer, wann, wo);
- Krisensitzung operativer Krisenstab;
  - Situation erfassen;
  - Schadenausmaß feststellen;
  - Sofortmaßnahmen zur Schadensbegrenzung;
  - Maßnahmen zur Sicherung des Geschäftsbetriebs (Notfallpläne aktivieren);
  - Beschlussfassung/Empfehlung von weiteren Aktivitäten für den strategischen Krisenstab (Entscheidungsvorlagen);
- Alarmierung des strategischen Krisenstabs;
- Krisensitzung strategischer Krisenstab;
  - Bericht über Situation und Schadensausmaß durch operativen Krisenstab;
  - Unterbreitung von Entscheidungsvorlagen durch operativen Krisenstab;
  - Beschlussfassung für Sofortmaßnahmen zur Schadensbegrenzung und zur Unternehmenssicherung;
- Steuerung der Öffentlichkeitsarbeit;
- Umsetzung und Steuerung von Maßnahmen durch operativen Krisenstab;
  - Koordination der Notfallaktivitäten;
  - Statusmeldungen;
  - Umsetzung von Öffentlichkeitsarbeit;
  - Beschlussfassung und Empfehlung weiterer Maßnahmen;
  - Feststellung des Endes der Notfallsituation;
- Deklaration des Endes der Notfall-, K-Fall-Situation durch den operativen Krisenstab, nach Beschluss durch den strategischen Krisenstab.

7.7.8 Ausfall des Host, des Rechenzentrums

Verfahren wie bei Ausfall Datenübertragung intern, zum Rechenzentrum, zu den Kunden.

7.7.9 Verstrahlung, Kontamination, Pandemie

Ablauf wie bei Brand (Nichtzutreffendes aus der Liste entfällt, Notwendiges ist entsprechend mit einzufügen).

Generell müssen hier aber zusätzliche Aspekte (Medikamente, Schutzkleidung, besondere Messgeräte, Medikamente, zugeschnittene Einsatzpläne von Personen) mit einbezogen werden, weil nicht nur das Unternehmen, sondern eine Region mit der Zivilbevölkerung betroffen ist. Insbesondere, wenn es darum geht, den Betrieb weiterhin als Notbetrieb aufrechtzuerhalten.

7.7.10 Sabotage

Ablauf muss individuell vorgegeben werden. Grundsätzlich kann hier ebenfalls die Verfahrensweise wie bei Brand genommen werden, wobei der Schwerpunkt nun eher auf der polizeilichen Seite zu sehen ist. Bei der Feststellung von Sabotage ist situativ zu unterscheiden, ob eingeleitete Sofortmaßnahmen die Feststellung des Verursachers unmöglich machen; hier sind möglicherweise andere Maßnahmen und Vorgehensweisen angebracht. Primär ist sicherlich zuerst eine Schadensbegrenzung einzuleiten, die aber situativ unterschiedlich ausfallen kann.

7.7.11 Spionage

Ablauf muss individuell vorgegeben werden. Bei der Feststellung von Spionage gilt Gleiches wie bei Sabotage.

Kapitel 8
Präventiv-, Notfall-, K-Fall-Planung

8.1 Präventiv- und Ausfallvermeidungsmaßnahmen

8.1.1 Generelle Vorgehensweise

Durch Präventivmaßnahmen soll im Vorfeld ein möglicher Schaden verlagert (durch rechtliche Absicherung, z. B. den Abschluss von Verträgen bzw. SLAs, Versicherungen, …), der Eintritt eines Notfalls verhindert (durch technische Vorsorge, z. B. Backup-System, …) und/oder die Ausführung des Notfallplans ermöglicht werden (durch Hilfsmittel, z. B. Faxvordrucke, Checkliste, Formulare, etc.) (siehe Abb. 27).

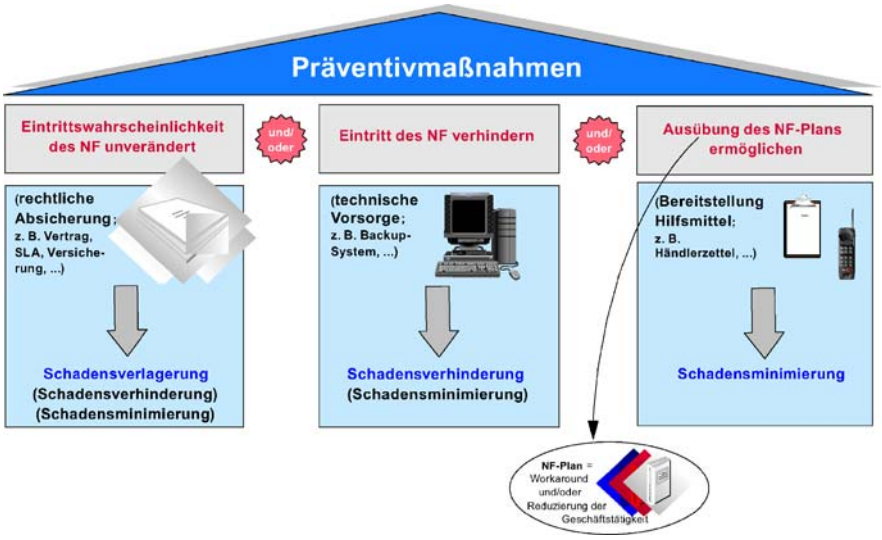


Abb. 27 Übersicht Präventivmaßnahmen

© Springer 2008

8.1.2 Präventivmaßnahmen, die einen möglichen Schaden verlagern

Im Vorfeld von Notfällen sind Präventivmaßnahmen möglich, die die Eintrittswahrscheinlichkeit eines möglichen Notfalles unverändert lassen, allerdings den Schaden im Not- und somit Schadensfall auf einen Dritten kraft Vertrag verlagern, z. B. durch:

- Service Level Agreement (SLA)/Vertrag; (zwecks Rechtssicherheit werden getroffene Vereinbarungen schriftlich in oben genannter Form fixiert);
- Versicherung;
- etc.

8.1.3 Präventiv- und Ausfallvermeidungsmaßnahmen, die den Eintritt des Notfalles verhindern

Zur Sicherstellung einer hohen Verfügbarkeit von Prozessen, Anwendungen und Systemen sind technische Präventivmaßnahmen erforderlich, die bei Störungen den Geschäftsbetrieb aufrechterhalten und den Eintritt des Notfalles verhindern, z. B.:

- Doppelung Hardware, Leitungen, etc.;
- Logging-, Datensicherungs-, Recovery-Verfahren;
- Verteilung von Systemen und Datenbeständen;
- Verschlüsselungsverfahren;
- Firewall/Zugriffsberechtigung und -kontrolle;
- Vorhaltung wichtiger Hardware und Ersatzteile;
- etc.

Die jeweils angewandten Maßnahmen sind in detaillierter Form Bestandteil des jeweiligen Betriebskonzeptes. Die Nutzung dieser technischen Vermeidungsmaßnahmen erfolgt im Störfall im Rahmen der normalen Linienkompetenz und bedarf in der Regel keiner Eskalation und keines Krisenstabes.

Eine Überprüfung der Präventivmaßnahmen ist bei der Neueinführung, mit jedem gravierenden Change oder mindestens einmal im Kalenderjahr sicherzustellen. Mit der Ersteinführung ist für die Überprüfung der Präventivmaßnahmen ein Testplan zu erstellen, der Bestandteil des Betriebskonzeptes ist. Der Testplan beschreibt die Durchführung und Protokollierung der Überprüfung (siehe Tabelle 31).

Tabelle 31 Präventive Überprüfungsverfahren

	Überprüfung von technischen Präventivmaßnahmen, die den Eintritt eines Notfalles verhindern:
Durchführung:	Regelmäßig durch verantwortlichen System-, Anwendungsbetreuer
Direkte Kontrolle:	Verantwortlicher Fachbereich, Qualitätsmanagement, zuständige Stabsstelle, Audit
Überwachung:	Revision im Rahmen von Prüfungsplänen oder situativ

8.1.4 Präventivmaßnahmen, die die Ausübung des Notfallplans ermöglichen

In den Notfallplänen sind die für deren Ausübung notwendigen Hilfsmittel aufgeführt, wie z. B.: Händlerzettel, Handys, Laptops, Schreibmaterial, Stempel, Telefonlisten und möglicherweise auch Notarbeitsplätze.

Eine Überprüfung dieser Hilfsmittel erfolgt im Rahmen von Notfall- und K-Fall-Übungen oder tatsächlich eingetretenen Notfällen bzw. K-Fällen.

8.1.5 Praktische Umsetzung und Anwendung

Generell muss bei den zu betrachtenden Systemen und IT-Komponenten zwischen dem Betrieb in Eigenverantwortung und dem Betrieb durch einen Dienstleister (z. B. ausgelagertes oder fremdes Rechenzentrum) unterschieden werden. Bei dem Eigenbetrieb sind die zu ergreifenden Maßnahmen unmittelbar selbst und in eigener Verantwortung umzusetzen und zu gewährleisten, wobei die Maßnahmen in einem Betriebskonzept zu dokumentieren sind. Bei dem Betrieb durch einen Dienstleister sind die Punkte ebenfalls mit der gleichen Wichtigkeit zu behandeln, hier sind Maßnahmen aber in einem Betriebskonzept und in einem Dienstleistungsvertrag (SLA) sehr detailliert und interpretationsfrei vorzugeben und es sind Kontrollstrukturen und Berichtswesen mit vorzusehen. Oftmals wird hier der Quasistandard ITIL (IT-Infrastruktur Library) genutzt.

Zu beachten ist auch, dass die ergriffenen Maßnahmen immer im Verhältnis Kosten zu potenziellem Schaden gesehen und bewertet werden müssen.

8.1.6 Bestehende Grundsicherheit in technischen Räumen

Bei der Installation von Systemen in technischen Räumen (Rechenzentrum, Serverräume, Technikräume) kann generell davon ausgegangen werden, dass eine unterbrechungsfreie Stromversorgung (USV) und eine Notstromversorgung (Notstromdiesel) zur Verfügung stehen. Ebenfalls sind diese Räume standardmäßig klimatisiert sowie mit entsprechenden Sicherungsmaßnahmen, wie CO_2-Flutung des Doppelbodens, Wassermelder, Rauchmelder, Sprinkler mit Vorflutung, Überwachungs-, Einbruchalarm- und Zugangskontrollsystemen, ausgestattet.

Die technischen Einrichtungen werden überwacht, regelmäßig geprüft und gewartet.

Generell müssen produktive IT-Komponenten und Systeme immer in gesicherten Räumen betrieben werden, wobei technische Räume unbedingt zu bevorzugen sind.

8.1.7 Maßnahmen in der Projektarbeit

Im Rahmen der Projektarbeit ist in der Phase Anforderungs-Analyse/Lösungsentwurf zu überprüfen, ob und welche Präventiv- und Ausfallvermeidungsmaßnahmen für Anwendungen, Systeme und IT-Infrastruktur vorzusehen sind und welche Kosten hierdurch entstehen. Bei erheblichen Kosten ist der betriebswirtschaftliche Nutzen, bzw. bei gesetzlichen Anforderungen der notwendige Erfüllungsgrad festzustellen. Als Ergebnis sind in Abstimmung mit dem Auftraggeber die umzusetzenden Präventiv- und Ausfallvermeidungsmaßnahmen festzulegen und im Fachkonzept zu dokumentieren; hier sollte auch genau begründet werden, welche Maßnahmen nicht umgesetzt werden. Falls keine Maßnahmen notwendig sind oder auf diese verzichtet wird, so ist dieser Sachstand mit Begründung ebenfalls im Fachkonzept zu dokumentieren.

8.1.8 Maßnahmen in der Linienaufgabe

Falls aufgrund eines Ereignisses oder durch neue Erkenntnisse Schwachstellen erkannt werden, die durch Präventiv- oder Ausfallvermeidungsmaßnahmen abgestellt werden können, so sind vom zuständigen Prozess-, Anwendungs- oder Systemverantwortlichen Vorschläge zu erarbeiten und die Kosten aufzuzeigen. Bei erheblichen Kosten ist der betriebswirtschaftliche Nutzen, bzw. bei gesetzlichen Anforderungen der notwendige Erfüllungsgrad festzustellen. Als Ergebnis sind in Abstimmung aller Beteiligten die umzusetzenden Präventiv- und Ausfallvermeidungsmaßnahmen festzulegen und zu protokollieren. Falls keine Maßnahmen notwendig sind oder auf diese verzichtet wird, so ist dieser Sachstand mit Begründung ebenfalls zu dokumentieren.

8.1.9 Verfügbarkeitsklasse

Auf Basis der Skalenwerte für Verfügbarkeit werden hier die Kategorien A1 bis A4 präzisiert.

Kategorie A1 hat keine nennenswerten Anforderungen an die Verfügbarkeit und fasst die IT-Infrastruktur, Systeme und Anwendungen zusammen, die nicht in die anderen drei Kategorien eingeordnet sind. Als Empfehlung sollte die Verfügbarkeit pro Jahr mindestens 90% betragen und der Einzelausfall nicht länger als fünf Tage dauern.

Die Kategorie A2 hat niedrige Anforderungen an die Verfügbarkeit. Die Anwendung selbst kann im Einzelfall bis zu zwei Tage ausfallen. Die normale Verfügbarkeit pro Jahr sollte aber mindestens 95% betragen, d. h. bei 250 Arbeitstagen pro Jahr dürfen die Systeme in der Summe der Ausfälle bis zu zwölf Tage

nicht zur Verfügung stehen. Zur Sicherung der Datenintegrität sind Datensicherungs- und Recovery-Prozeduren vorzusehen.

Die Kategorie A3 bedeutet eine normale Verfügbarkeit, wobei pro Einzelausfall die Nichtverfügbarkeit bis zu einem Tag toleriert und verkraftet werden kann. Die normale Verfügbarkeit pro Jahr sollte aber mindestens 98% betragen, d. h. bei 250 Arbeitstagen pro Jahr dürfen die Systeme in der Summe der Ausfälle bis zu fünf Tage nicht zur Verfügung stehen. Folgende Sicherungsmaßnahmen sind i. d. R. vorgesehen:

- Standardmäßige Datensicherungsverfahren sowie Logging/Recovery;
- Vorhaltung wichtiger Verschleißteile oder Ersatzsysteme;
- Serviceverträge mit Lieferanten, die eine Ersatzteilbeschaffung oder Fehlerbehebung in einer vertretbaren Zeit gewährleisten;
- n + 1-Technik (ein zusätzlicher Server, der die Arbeit übernimmt, wenn ein anderer ausfällt);
- Plattenspiegelung (RAID).

Die Kategorie A4 bedeutet, dass ein Einzelausfall bis zu zwei, max. vier Stunden toleriert und verkraftet werden kann. Die Verfügbarkeit pro Jahr muss mindestens bei 99,5 % liegen. Eine unterbrechungsfreie Verfügbarkeit kann mit folgenden Maßnahmen erreicht werden:

- Backup von IT-Systemen (cold, warm, hot standby);
- Doppelung von IT-Infrastruktur und Leitungen;
- Verteilung von IT-Systemen und Datenbeständen über verschiedene Lokationen;
- Bereitschaftsdienst von Systembetreuern und Technikern vor Ort;
- Bereithaltung ausreichender Ersatzteile und Hardware;
- Serviceverträge mit Lieferanten (hot-standby-Bereitschaft);
- Als Ergänzung oder in Kombination können die Maßnahmen der anderen Kategorie mit einbezogen werden.

Zusätzlich sind bei Systemen, die nicht in Eigenverantwortung betrieben werden, bzw. von externen Dienstleistern zur Verfügung gestellt werden, folgende Punkte zu beachten:

- Berücksichtigung von Störungs-, Notfall- und K-Fall-Maßnahmen im SLA;
- Schaffung einer klaren Rechtslage zu den Themen Haftung und Gewährleistung;
- Beschreibung der Verfahren für Eskalation, Fehlerlokalisierung, Behebung und Wiederanlauf in Störungs-, Notfall- und K-Fall-Situationen im Betriebskonzept. Testverfahren zur Überprüfung der Ausfallvermeidungsmaßnahmen;
- Klare Darstellung der Pflichten des Auftraggebers zur Erfüllung des Vertrages; welche Umsetzungsmaßnahmen sind hier notwendig?
- Überprüfung, ob es weitere Dienstleister gibt, deren Produkte alternativ in Anspruch genommen werden können.

8.1.10 Überprüfung von Präventiv- und Ausfallvermeidungsmaßnahmen

Zur Überprüfung von Präventiv- und Ausfallvermeidungsmaßnahmen sind Prüfkonzepte zu entwickeln und Messgrößen vorzugeben, über die dann im Rahmen regelmäßiger Tests die Funktionstüchtigkeit nachgewiesen werden kann. Diese Prüfkonzepte sind als fester Bestandteil in das Betriebskonzept zu integrieren.

Die Tests sind an produktiven Systemen vorzunehmen. Bei einer Gruppe gleichartiger Systeme kann auch ein Stellvertretertest durchgeführt werden, wobei rollierend mit jedem Test ein anderes System überprüft wird (siehe Tabelle 32). Wenn die Gruppe größer ist, so sind stichprobenhaft mehrere Systeme bei einem Test zu überprüfen. Verteilt sich diese Gruppe über mehrere Standorte, so sind die Stichproben entsprechend auch verteilt vorzunehmen.

Tabelle 32 Stichproben bei gleichen Systemen

Anzahl gleichartiger Systeme	Anzahl zu testender Systeme
1 bis 5	1
5 bis 10	2
11 bis 20	3
über 20	pro weitere 20 ein zusätzliches System

8.1.11 Versicherung

Zur Abdeckung von finanziellen und materiellen Risiken ist auch zu überprüfen, ob entsprechende Versicherungen abzuschließen sind. Bei vorhandenen Versicherungen ist durch Veränderung oder auch durch Wegfall von Risiken eine Anpassung notwendig. Eine Überprüfung sollte mindestens einmal jährlich stattfinden.

8.1.12 Checkliste zur Feststellung des Schutzbedarfs bei Präventiv- und Ausfallvermeidungsmaßnahmen

Durch die Vielschichtigkeit von Präventiv- und Ausfallvermeidungsmaßnahmen kann nur ein Template vorgegeben werden, das entsprechend angepasst und ergänzt werden muss. Diese Checkliste (siehe Tabelle 33) dient einerseits dazu, die Schutzbedarfsklasse und die entsprechenden Anforderungen zu definieren, und andererseits erkannte Defizite aufzuzeigen. Eine Schutzbedarfsklasse (S1–S4) ist aus den Klassifizierungen der Vertraulichkeit (C1–C4), der Integrität (I1–I4), der Verfügbarkeit (A1–A4), der Verbindlichkeit (B1–B4) und möglicherweise aus weiteren mit einzubeziehenden Faktoren zu bilden.

Tabelle 33 Checkliste Schutzbedarf bei Präventiv- und Ausfallvermeidungsmaßnahmen

	Bemerkung	Verant-wortlich
System:	Name des Systems, Typ	
Bewertung: Verfügbarkeit:	Bewertung: Vertraulichkeit C1 bis C4 Integrität I1 bis I4 Verfügbarkeit A1 bis A4 Verbindlichkeit B1 bis B4 Konkretisierung der notwendigen Verfügbarkeit in Prozent pro Jahr	
Ausfallverträglichkeit:	mögliche zu verkraftende Ausfallzeiten, Ausfallzeiten durch Wartung, Changes, Wiederanlaufzeit, Verlauf des Schadenspotenzials bei Überschreitung der verträglichen Ausfallzeiten.	
Schadenpotenzial:	Welcher Schaden kann entstehen? Hier sind Stück- bzw. Anzahl Geschäftsvorfälle sowie der Erlös zu berücksichtigen. Weiterhin sind auch Imageschäden, unmittelbare oder mittelbare Folgeschäden und Haftungs- und Gewährleistungsansprüche mit zu betrachten.	
Risiken:	Welche Risiken sind zusätzlich zu betrachten? Z. B. Personal-, Rechtsrisiken.	
Präventiv-, Ausfallvermeidungsmaßnahmen:	Feststellung, ob Präventiv-, Ausfallvermeidungsmaßnahmen notwendig sind. Wenn nein, dann ist eine Begründung zu dokumentieren.	
Lokation/Benutzer	An welchen Orten befinden sich Benutzer?	
Anwendungen, die auf dem System laufen:	Name, Kurzbeschreibung Teil eines wichtigen Prozesses?	
Betriebskonzept:	Liegt ein Betriebskonzept vor oder wird ein Betriebskonzept mit den Themen Datensicherung/Recovery, IT-Security erstellt?	
Versicherungen:	Besteht ein besonderes Risiko, das versichert werden muss? Muss eine bestehende Versicherung angepasst werden? (Schwachstrom-, Betriebsausfallvers.)	
Bei SLAs:	• Vertragspartner • Leistungsbeschreibung • Hotline, Erreichbarkeit • Notfallanweisungen • Kontrollstrukturen zur Überwachung	
Ausfallmöglichkeiten, Schwachstellen:	• Welche Ausfälle sind zu betrachten? • Gibt es Besonderheiten, die zu beachten sind?	
Technische Möglichkeiten zur Ausfallvermeidung	Welche der Präventiv- und Ausfallvermeidungsmaßnahmen sind angemessen, betriebswirtschaftlich vertretbar und auch vorgesehen? Spiegelung, n + 1-Technik, RAID?	

Tabelle 33 (Fortsetzung)

	Bemerkung	Verant-wortlich
Benötigte Ressourcen:	• Personalressourcen für Wartung, Überprüfung, • Hardware, Ersatzteile, Wiederbeschaffung, • Software, Master-CD, • Zugriffsberechtigung, • Kosten	
Zeit-, Umsetzungsplan:	• Installation, Implementierung, • Schulung, Einweisung, • Überführung in die Produktion	
Prüfverfahren:	• Prüfkonzept mit Festlegung von Messgrößen, • Bei gleichartigen Systemen sind Pläne für Stell-vertretertests vorzugeben, • Darstellung der Risiken aus der Überprüfung	
Einstufung in die Schutzbedarfsklasse: S1–S4	Festlegen der Schutzbedarfsklasse • S1: geringer Schutzbedarf • S2: niedriger Schutzbedarf • S3: normaler Schutzbedarf • S4: hoher Schutzbedarf	

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

8.1.13 Checkliste zur Überprüfung von Ausfallvermeidungsmaßnahmen

Für die Überprüfung ist eine Checkliste (siehe Tabelle 34) zu erstellen, die die Messgrößen enthält und die den Ablauf der Überprüfung beinhaltet. Die Checkliste kann als Ergänzung zu einem Abschlussprotokoll genommen werden. Im Folgenden ist ein Entwurf einer Checkliste aufgeführt, die als Muster verwendet und angepasst werden kann.

Tabelle 34 Checkliste Überprüfung Ausfallvermeidungsmaßnahmen

1	Protokollant/Prüfer:	Name: OE:
2	Datum und Uhrzeit der Überprüfung:	Datum: Uhrzeit:
3	Systemname, -Typ	Welche Systeme, Stellvertretertests?
4	Lokation, Standort	Rechenzentrum, Serverraum, Technikraum, Dienstleister
5	Geschäftsprozess, Anwendung:	Welche Anwendungen sind betroffen?
6	Betroffene Benutzer:	Benutzerkreis feststellen und frühzeitig involvieren und benachrichtigen.
7	Testablauf:	Datensicherung; Initiierung Ausfall, Störung; Überprüfung der Ausfallvermeidungsmaßnahmen; Wiederanlauf und Übergang in Normalbetrieb; Überprüfung ordnungsgemäße Funktion des Systems und der Datenkonsistenz.

Tabelle 34 (Fortsetzung)

8	Ziele bzw. zu erwartende Ergebnisse (Messgrößen):	Switch auf Backup ordnungsgemäß; Alarmierung der Überwachungseinheit ordnungsgemäß; Übergang in Normalbetrieb einwandfrei; Rücksicherung einwandfrei und in vertretbarer Zeit; Datenkonsistenz ist überprüft und fehlerfrei.	
9	Risiken, die sich aus Überprüfung/Test ergeben:	Was passiert, wenn der Wiederanlauf fehlschlägt? Stehen die System- und Anwendungsverantwortlichen zur Verfügung? Wie lange dauert ein Kaltstart, eine Neuinitiierung des Systems? Gibt es Hardwareersatz?	
10	Notwendige Personen:	NF-Manager: Tel.: Anwendungsbetreuer: Tel.: Systembetreuer: Tel.: Mitarbeiter aus FB Tel.: Wichtig ist die frühzeitige Einbindung der tangierten Personen	OE: Vertreter: OE: Vertreter: OE: Vertreter: OE: Vertreter:
11	Bemerkungen:	Eintrag von Bemerkungen und Besonderheiten, die zu berücksichtigen sind.	

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

8.2 Notfall- und Kontinuitätspläne

8.2.1 Inhalte des Notfallhandbuches

Das Notfallhandbuch soll in erster Linie über die in Notfällen zu treffenden Maßnahmen und die einzuhaltenden Verfahren informieren. Darüber hinaus sind inhaltlich die Präventivmaßnahmen, die für den Notfall- und Kontinuitätsplan notwendig sind, sowie Anweisungen für den Wiederanlauf, nach Ende eines Notfalls oder K-Falls zur Sicherstellung der Datenintegrität, Bestandteil des Notfallhandbuchs. Das Handbuch beinhaltet keine Präventivmaßnahmen im Sinne der Ausfallvermeidung, keine Anweisung für Notfallauswertung und auch keine Hinweise für Notfallübungen. Die Zuständigkeit für diese Themen liegt beim Notfallmanager des jeweiligen FB und bei dem Security-Officer oder einer vergleichbaren Funktion wie z. B. einem IT-Security & Contingency Management.

8.2.2 Handhabung des Notfallhandbuches (IT-Krisenstab, Notfallpläne, Anhang)

Das Notfallhandbuch ist von den Mitarbeitern der betroffenen Organisationseinheiten in regelmäßigen Abständen durchzuarbeiten, so dass bei Eintritt eines

Notfalls der Umgang mit dem Handbuch vertraut ist und die erforderlichen Maßnahmen unverzüglich ergriffen werden können. Darüber hinaus sind die Aktualität, Zuständigkeiten und Querverbindungen zu überprüfen. Verbesserungen sind durch den entsprechenden Notfallmanager des jeweiligen Fachbereiches zeitnah einzuarbeiten.

Bei Eintritt eines Notfalls sind die Maßnahmen der entsprechenden Notfallpläne anzuwenden. Darüber hinaus sind die Querverbindungen zu überprüfen und es ist zu klären, wer bei Ausfall einer Anwendung, einer Schnittstelle, einer Organisationseinheit oder eines Produkts noch betroffen und zu informieren ist.

Nach Beendigung des Notfalls sind die für die Nachbearbeitung notwendigen Unterlagen, z. B. um Ergänzungen, Korrekturen oder Neuerstellung von Notfallplänen zu veranlassen, dem Notfallmanager im FB und dem Security-Officer bzw. einer zentralen Sicherheitsfunktion nachzureichen, sofern diese nicht schon in deren Besitz gelangt sind.

8.2.3 Ziele des Notfallhandbuches

Ziel des Notfallhandbuches ist die Sicherstellung eines geordneten Vorgehens (siehe Abb. 28) im Notfall zwecks Schadensminimierung und schnellstmöglicher Wiederherstellung der Funktionsfähigkeit von Prozessen, Systemen und Anwendungen. Bestandteil dieses Handbuches sind auch Maßnahmen, die ergriffen werden müssen, um einen geregelten Wiederanlauf zu gewährleisten.

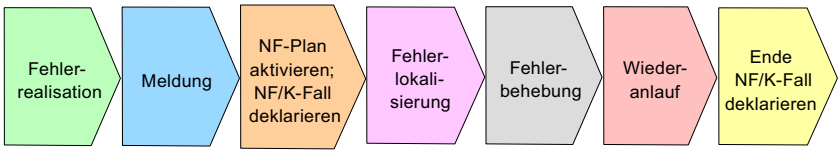


Abb. 28 Notfall- und K-Fall-Prozess

8.2.4 Praktische Anwendung und Umsetzung

8.2.4.1 Feststellung der Notwendigkeit von Notfall- und Kontinuitätsplan

Generell muss bei den zu betrachtenden Prozessen/Anwendungen zwischen dem Betrieb in Eigenverantwortung und dem Betrieb durch einen Dienstleister (z. B. Rechenzentrum) unterschieden werden. Bei dem Eigenbetrieb sind die zu ergreifenden Maßnahmen unmittelbar selbst und in eigener Verantwortung umzusetzen und zu gewährleisten, wobei die Maßnahmen in der Prozessdokumentation (z. B. ARIS) sowie für jede Anwendung in einem Betriebskonzept zu dokumentieren

sind. Bei dem Betrieb durch einen Dienstleister sind die Punkte ebenfalls mit der gleichen Wichtigkeit zu behandeln; hier sind Maßnahmen interpretationsfrei in der Prozessdokumentation, in den Betriebskonzepten und im Dienstleistungsvertrag (SLA) vorzugeben. Darüber hinaus sind Kontrollstrukturen und Berichtswesen vorzusehen. Zu beachten ist auch, dass die ergriffenen Maßnahmen immer im Verhältnis Kosten zu potenziellem Schaden gesehen und bewertet werden.

Maßnahmen in der Projektarbeit

Im Rahmen der Projektarbeit ist in der Phase Anforderungs-Analyse/Lösungsentwurf zu überprüfen, ob und welche Notfall- und Kontinuitätsmaßnahmen für Prozesse/Anwendungen vorzusehen sind und welche Kosten hierdurch entstehen. Bei erheblichen Kosten ist der betriebswirtschaftliche Nutzen, bzw. bei gesetzlichen Anforderungen der notwendige Erfüllungsgrad festzustellen. Als Ergebnis sind in Abstimmung mit dem Auftraggeber die umzusetzenden Maßnahmen festzulegen und im Fachkonzept zu dokumentieren; hier sollte auch genau begründet werden, welche Maßnahmen nicht umgesetzt werden. Falls keine Maßnahmen notwendig sind oder auf diese explizit verzichtet wird, so ist dieser Sachstand mit Begründung ebenfalls im Fachkonzept zu dokumentieren. Aufbauend auf Erkenntnisse der Phase Analyse/Entwurf ist der Notfall- und Kontinuitätsplan in der Projektphase Realisierung/Test zu erstellen.

Maßnahmen in der Linienaufgabe

Falls aufgrund eines Ereignisses oder auf anderen Wegen Schwachstellen erkannt werden, die durch einen Notfall- und Kontinuitätsplan abgestellt werden können, so sind vom zuständigen Prozess-, Anwendungs- oder Systemverantwortlichen Vorschläge zu erarbeiten und die Kosten aufzuzeigen. Bei erheblichen Kosten ist der betriebswirtschaftliche Nutzen, bzw. bei gesetzlichen Anforderungen der notwendige Erfüllungsgrad festzustellen. Als Ergebnis sind in Abstimmung aller Beteiligten die umzusetzenden Maßnahmen festzulegen und zu protokollieren. Falls keine Maßnahmen notwendig sind oder auf diese explizit verzichtet wird, so ist dieser Sachstand mit Begründung ebenfalls zu dokumentieren.

Feststellung der Schutzbedarfsklasse bei Prozessen und Anwendung

Für Daten und Anwendung ist die Vertraulichkeit, Integrität, Verbindlichkeit und insbesondere die Verfügbarkeit zu bewerten. Diese Aspekte spiegeln sich auch in der Wichtigkeit der Prozesse und Anwendungen wider, wobei für jeden Prozess, jede Anwendung eine Kategorisierung in die Schutzklassen S1 bis S4 (gering, niedrig, mittel, hoch) vorzunehmen ist.

Für die Ausfallverträglichkeit jedes Prozesses, jeder Anwendung ist durch den Fachbereich die Verfügbarkeit festzulegen. Die Verfügbarkeit wird in die Kategorien A1 bis A4 (gering, niedrig, normal, hoch) eingestuft.

Die Sicherstellung einer angemessenen Verfügbarkeit des Prozesses/der Anwendung kann mit folgenden Maßnahmen erreicht werden:

- Standardmäßige Datensicherungsverfahren sowie Logging/Recovery;
- Einsatz von Hochverfügbarkeitshard- und -software;
- Verteilung von Anwendungen und Datenbeständen;
- Technische Maßnahmen in Absprache mit den Systembetreuern, -betreibern;
- Bereitschaftsdienst von Anwendungsbetreuern;
- Wartungs- und Serviceverträge mit Lieferanten und Vereinbarung entsprechender Reaktions- und Fehlerbehebungszeiten.

Folgende Punkte sind zusätzlich bei Prozessen/Anwendungen zu berücksichtigen, die durch externe Dienstleister betrieben oder zur Verfügung gestellt werden:

- Berücksichtigung von Störungs-, Notfall- und K-Fall-Maßnahmen im SLA;
- Schaffung einer klaren Rechtslage zu den Themen Haftung und Gewährleistung;
- Beschreibung der Verfahren für Eskalation, Fehlerlokalisierung, Behebung und Wiederanlauf in Störungs-, Notfall- und K-Fall-Situationen im Betriebskonzept;
- Testverfahren zur Überprüfung der Ausfallvermeidungsmaßnahmen;
- Klare Darstellung und Umsetzung der Pflichten des Auftraggebers zur Erfüllung des Vertrages;
- Überprüfung, ob es weitere Dienstleister gibt, deren Produkte alternativ in Anspruch genommen werden können.

8.2.4.2 Checkliste für die Erstellung eines Notfallplans

Durch die Vielschichtigkeit von Notfallplänen kann nur ein Template (siehe Tabelle 35) als Basis vorgegeben werden, das entsprechend ergänzt und angepasst werden muss. In vielen Fällen existieren aber schon Notfall- und Kontinuitätspläne, wobei diese entsprechend genommen und überarbeitet werden können.

Tabelle 35 Checkliste Notfall-, Kontinuitätsplan

1	Prozess/Anwendung:	Name des Prozesses, der Anwendung
2	Bewertung/Einstufung:	Bewertung: • Vertraulichkeit C1 bis C4 • Integrität I1 bis I4 • Verfügbarkeit A1 bis A4 • Verbindlichkeit B1 bis B4
3	Ausfallverträglichkeit:	Einschätzung der Ausfallzeiten: • Wie lange ohne Aktivitäten (Wartestatus der Benutzer)? • Ab wann greift ein Notfall-, Kontinuitätsplan? • Ab wann ist der operative Krisenstab zu informieren? • Ab wann ist der strategische Krisenstab zu informieren?

Tabelle 35 (Fortsetzung)

4	Schadenspotenzial:	Verlauf des Schadenspotenzials mit fortschreitender Zeit: • Schaden nach 2 Std.; • Schaden nach 4 Std.; • Schaden nach einem Tag; • Schaden nach zwei Tagen; • Schaden nach einer Woche.
5	Notfall-, Kontinuitätsplan:	Reicht ein Notfallplan als Erstmaßnahme zur Schadensbegrenzung oder ist ein Workaround als Kontinuitätsplan notwendig, um den Prozess in einer steuerbaren Form aufrechtzuerhalten?
6	Verantwortlicher:	FB: Name: Wer ist Betreiber (Owner) des Prozesses, der Anwendung? Wer trägt die juristische Verantwortung?
7	Beschreibung:	Kurzbeschreibung des betriebswirtschaftlichen Ablaufs und der Schnittstellen.
8	Inhalte des Notfall-, Kontinuitätsplans: (Bei keinen Notfallmaßnahmen ist hier die Begründung zu dokumentieren)	Fragestellungen zur Gestaltung des Notfallplans: • Woran ist der Notfall zu erkennen (Kriterien) und welche Maßnahmen sind zu ergreifen? • Wer ist zur Fehlerlokation, Fehlerbehebung direkt zu informieren (Systembetreuer, Dienstleister)? • Wie sieht das Eskalationsverfahren zur Notfallbewältigung intern aus? Wann und wer ist zu informieren? • Ist die Öffentlichkeit, sind Kunden und Geschäftspartner zu informieren? • Beschreibung des Workaround (Workflow, Kommunikationswege, Priorisierung von Geschäftsvorfällen); • Welche Mittel sind für den Workaround vorzuhalten (Präventivmaßnahmen)? • Welche Ressourcen, Ersatzmaschinen, Kommunikationsmittel und Räumlichkeiten sind notwendig? • Sicherstellung des Wiederanlaufs; • Nacherfassung von Geschäftsvorfällen; • Überprüfung der Datenkonsistenz; • Überführung in den Normalbetrieb (Ende des Notfalls).
9	Betroffene OEen:	Welche OEen, welche internen und externen Benutzer sind im Notfall betroffen?
10	Schwachstellen-Analyse und Risikoeinschätzung: Schutzbedarf:	In Zusammenarbeit mit dem FB, den Anwendungs- und Systembetreuern sowie mit dem Security-Officer ist eine Risikoeinschätzung durchzuführen (Smart-Scan, FMEA). Festlegen der Schutzbedarfsklasse: • S1: geringer Schutzbedarf; • S2: niedriger Schutzbedarf; • S3: mittlerer oder normaler Schutzbedarf; • S4: hoher Schutzbedarf.

Tabelle 35 (Fortsetzung)

11	Verantwortliche und notwendige Personen: Namen, OE, Funktion	NF-Manager: OE: Tel.: Vertreter: Anwendungsbetreuer: OE: Tel.: Vertreter: Systembetreuer: OE: Tel.: Vertreter: Mitarbeiter: OE: Tel.: Vertreter:
	Operativer Krisenstab:	Name: Bereichs- oder Abt.-Leiter FB/OE: Tel.: Vertreter: Name: Bereichs-, Abt.-Leiter ORG/OE: Tel.: Vertreter:
	Strategischer Krisenstab:	Name: Geschäftsführer, Vorstand Tel.: Vertreter: Name: Vorstand des betroffenen FB Tel.: Vertreter: Name: Vorstand Informatik, Revision, Recht, Verwaltung Tel.: Vertreter: Name: notwendige Bereichsleiter Tel.: Vertreter:
12	Wiederanlauf:	Name: OE: Tel.: (notwendige und verantwortliche Person für die Nacherfassung und Prüfung auf Datenintegrität)
13	Bemerkungen:	

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

Jeder neu erstellte Notfallpan wird bei der Produktionsübergabe vom zuständigen Notfallmanager in eine zentrale Notfall-DB eingestellt. Ebenfalls wird jeder aktualisierte Notfallplan im Rahmen des Changeprozesses eingepflegt, wobei der vorhergehende Notfallplan historisiert wird. Die Notfall-DB wird vom Security-Officer oder einer Funktion IT-Security & Contingency Management zur Verfügung gestellt.

8.2.5 Notfall- und K-Fall-Übungen

Unterscheidung Notfall-/K-Fall-Übung

Bei der Betrachtungsweise der Notfall- bzw. K-Fall-Übungen wird der Fokus auf die Prozesse, Anwendungen und Systeme gelegt, wobei in diesem Kontext zwischen zwei Übungsarten unterschieden wird:

- Notfallübungen zur Überprüfung eines Notfallplans in der Praxis, wobei anhand von Vorgaben und Vorbereitungen, der Durchführung und der Nachbearbeitung die Funktionalität des Notfallplans und dessen Umsetzung getestet wird. *Beispiele: Ausfall Wertpapierhandelssystem, Zahlungsverkehrssystem,etc.*

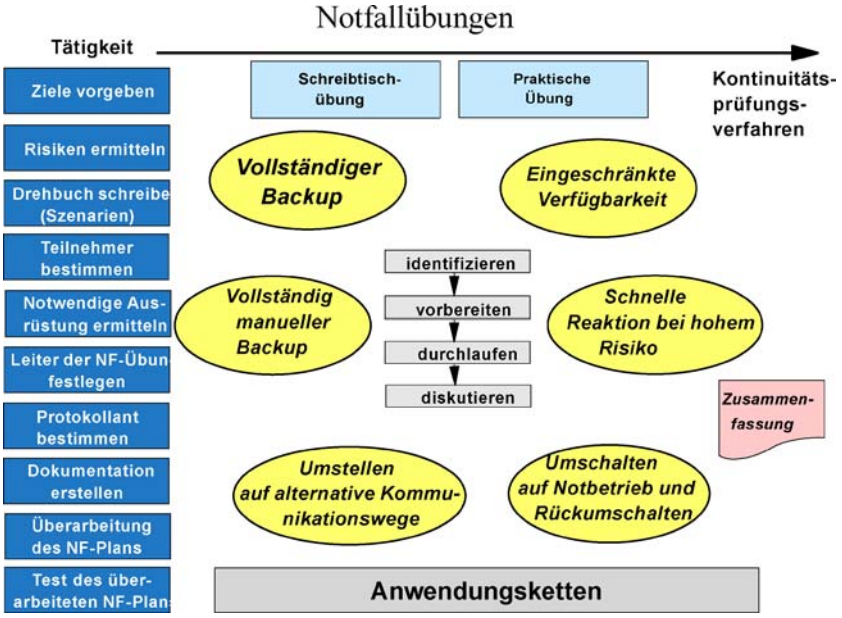


Abb. 29 Möglichkeiten von Notfallübungen

- K-Fall-Übungen zur Überprüfung des komplexen Zusammenspiels mehrerer Notfall-, Kontinuitätspläne und Sicherungsmaßnahmen in der Praxis, wobei von einem K-Fall-Szenario ausgegangen wird. *Beispiele: Brand, Hochwasser, Bombenanschlag, ...*

Innerhalb dieser zwei Übungen ist zu differenzieren zwischen unangekündigten und angekündigten Übungen sowie zwischen reinen Schreibtisch- oder sog. Trockenübungen und praktischen Übungen. Bei technischen Notfallübungen gibt es weitere Unterscheidungen und Varianten bei der Durchführung (siehe Abb. 29).

Häufigkeit der Übungen

Notfall- und K-Fall-Übungen sind entsprechend den gesetzlichen Vorgaben regelmäßig durchzuführen. Für Prozesse/Anwendungen mit dem Schutzbedarf S4 „hoch“ ist eine Notfallübung pro Jahr zu empfehlen. Bei Prozessen/Anwendungen mit dem Schutzbedarf S3 „mittel“ ist alle zwei Jahre eine Notfallübung zu empfehlen.

Um die Penetranz der Notfall- und K-Fall-Übungen auf ein vertretbares Maß zu beschränken, ist anzustreben, dass jeder tangierte Mitarbeiter nach Möglichkeit nur einmal im Jahr an einer Notfallübung teilnimmt. Die Planung und Koordination obliegt dem Security-Officer oder einer Funktion „IT-Security & Contingency Management“ in Abstimmung mit den tangierten FB.

8.2.6 Notfallübungen

Überblick über die Planung, Durchführung und Nachbereitung von Notfallübungen

Bei der Planung und Durchführung von Notfallübungen, zur Aufrechterhaltung des Geschäftsbetriebs und zur Überprüfung der Inhalte und des Umgangs mit den Notfallplänen, gibt es folgende Schritte:

- Feststellung möglicher Risiken, die durch die Notfallübung verursacht werden können;
- Überprüfung, dass alle involvierten Personen im Besitz des aktuellen Notfallplans sind;
- Aufbau einer Checkliste für die Durchführung der Notfallübung mit Festlegung Ort, Zeit, Teilnehmer, Ausfallszenario sowie der zu erwartenden Ergebnisse aus der Übung (Festlegen von Messgrößen und Erwartungswerten); wichtig ist vorab die Klärung der Zuständigkeit und Kompetenzen (siehe Tabelle 36);
- Durchführung der Notfallübung: Prüfen der spezifischen Pläne und Prozeduren, einschließlich aller Schnittstellen und Abhängigkeiten, und Dokumentation der Ergebnisse;
- Wiederanlauf oder Backup sicherstellen;
- Nachbereitung der Notfallübung;
- Vergleich der erzielten Ergebnisse mit den erwarteten Ergebnissen (festgelegte Messgrößen);
- Festlegung notwendiger Maßnahmen aufgrund erkannter Schwachstellen, z. B. Überarbeitung der Notfallpläne wegen Lücken- oder Fehlerhaftigkeit;
- Initiierung und Umsetzung der Sofortmaßnahmen mit Vorgabe eines Zeitrahmens;
- Überprüfung durch den zuständigen Notfallmanager und den Security-Officer bzw. durch das IT-Security & Contingency Management, ob die Maßnahmen terminlich und inhaltlich umgesetzt und realisiert wurden.

Zuständigkeiten für NF-Übungen:

Tabelle 36 Zuständigkeit Notfallübung

	NF-Übungen:
Durchführung:	Security-Officer, bzw. IT-Security & Contingency Management in Verbindung mit den betroffenen FB (Notfallmanager) sowie den zuständigen System- und Anwendungsbetreuern oder auch ext. Dienstleistern
Direkte Kontrolle :	Verantwortlicher Fachbereich, Qualitätsmanagement, zuständige Stabsstelle
Überwachung:	Revision

Durchführung von Notfallübungen

Notfallübungen sind eigenständig vom verantwortlichen Fachbereich vorzunehmen, wobei zur Beratung und Unterstützung das IT-Security & Contingency-Management sowie die entsprechenden Anwendungs- und Systembetreuer eingebunden werden. Anhand der Schutzbedarfsklasse sind die notwendigen Test einzuplanen und durchzuführen (siehe Tabelle 37).

Tabelle 37 Testzyklus

Schutzbedarfsklasse	Testzyklus
S1 (gering)	kein Test notwendig
S2 (niedrig)	Test bei Neuinstallation oder bei Veränderung
S3 (mittel)	Bei Neuinstallation oder Veränderungen, spätestens aber alle zwei Jahre (Empfehlung)
S4 (hoch)	Bei Neuinstallation oder bei Veränderungen, spätestens aber einmal pro Jahr (Empfehlung)

Für die Durchführung von Notfallübungen sind Prüfkonzepte zu entwickeln und Messgrößen vorzugeben, über die dann im Rahmen regelmäßiger Übungen die Funktionstüchtigkeit nachgewiesen werden kann. Diese Prüfkonzepte sind als feste Bestandteile in das Betriebskonzept zu integrieren. Notfallübungen sind im laufenden Geschäftsprozess und an produktiven Systemen durchzuführen.

Checkliste für die Planung von Notfallübungen

Für die Planung einer Notfallübung kann die folgende Checkliste als Template genommen und den Bedürfnissen angepasst werden.

Tabelle 38 Checkliste „Notfallübung“

1	Protokollant:	Name: OE:
2	Datum und Uhrzeit der angesetzten Notfallübung:	Datum: tt.mm.jj von: *hh:mm* bis: *hh:mm*
3	Leiter der Notfallübung:	Notfallmanager; Moderation durch Security-Officer.
4	Betroffener Notfallplan:	Prozess, Anwendung, System, Plattform?
5	Betroffene OEen:	• Welche Mitarbeiter nehmen an der Übung teil? • Ist Rechenzentrum oder ext. Dienstleister mit einzubinden?
6	Erstellung eines Drehbuchs:	• Art der Notfallübung festlegen (Schreibtischtest, Systeme abschalten, etc.); • Vorgehensweise innerhalb der Übung; • Aufgabenverteilung; • Verantwortlichkeiten; • Termine.

Tabelle 38 (Fortsetzung)

7	Ziele bzw. zu erwartende Ergebnisse:	Anhand welcher Kriterien ist der Erfolg der Notfallübung messbar? Mess- und Erwartungsgrößen festlegen	
8	Risiken der Übung:	Was für Schäden können durch die Notfallübung ausgelöst werden? Müssen hier besondere Vorkehrungen getroffen werden?	
9	Abstimmung mit OEen erfolgt? Vorankündigung der Übung? Wenn ja, wie lange vorher?	□ Ja □ Keine Ankündigung □ 4 Wochen vorher	□ Nein □ 1 Woche □ Andere Vorankündigung
10	Art der Übung:	□ Schreibtisch-Übung/Workshop □ Praktische Übung vor Ort □ Sonstige (Art der Übung festlegen)	
11	Räumlichkeiten:	Lokation, Gebäude, Etage, Raum	
12	Notwendige Ausrüstung:	□ Overhead □ Moderatorenkoffer □ Beamer	□ Flipchard □ Pinnwand □ Sonstiges
13	Notwendige Personen (Name, OE, Funktion): Operativer Krisenstab: Anmerkung: Der strategische Krisenstab wird in eine Notfallübung nicht mit einbezogen	NF-Manager: Tel.: Anwendungsbetreuer: Tel.: Systembetreuer: Tel.: Mitarbeiter FB Tel.: Name: Bereichsleiter des FB Tel.: Name: Tel.: Name: Tel.:	OE: Vertreter: OE: Vertreter: OE: Vertreter: OE: Vertreter: OE: Vertreter: OE: Vertreter: OE: Vertreter:
14	Zeitrahmen der Notfallübung:	Beginn: (welcher Zeitraum soll simuliert werden, z. B. 3 Tage im Zeitraffer?)	Ende:
15	Wiederanlauf: (notwendige und verantwortliche Personen)	Name: Tel.:	OE:
16	Bemerkungen:		

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

Erstellung eines Drehbuchs für eine Notfallübung

Für jede Notfallübung ist ein Drehbuch zu erstellen, das den Ablauf der Notfallübung minuziös beschreibt. Verantwortlich für die Erstellung und für die sachliche Richtigkeit des Drehbuchs ist der zuständige Notfallmanager im FB. Unterstützung und Beratung erfolgen durch die fachlich zuständigen Serviceeinheiten und durch den Security-Officer, bzw. durch das IT-Security & Contingency Management.

Bei der Gestaltung des Drehbuchs sind folgende Punkte zu betrachten und einzuarbeiten:

- Festlegung des Notfallszenarios, d. h. welcher Prozess, Teilprozess, welche Anwendung oder welches System soll gravierend gestört sein?
- Bestimmung des Personenkreises, der unmittelbar in die Planung einbezogen wird. Diese Personen sind entsprechend zur Geheimhaltung der Notfallübung selbst und deren Inhalt zu verpflichten.

Nun gilt es den Umfang der Notfallübung festzulegen, wobei Standort, Arbeitsplätze, Personen und weitere Fakten zu bestimmen sind. Hier ist auch zu klären, inwieweit das Notfallszenario simuliert wird, d. h. es werden Anwendungen, Prozesse in einen Zustand gebracht, die der tatsächlichen Notsituation entsprechen; dazu sind umfassende Absprachen mit den Systembetreuern, mit der Hausverwaltung und den Störungsstellen (UHD, Hotline, …) zu treffen, damit diese auf die Notfallübung vorbereitet sind. Weiterhin sind als Indiz für ein funktionierendes Notfallkonzept Messgrößen zu definieren, die während der Notfallübung überprüft und dann ausgewertet werden. Messgrößen können sein:

- Ist ein aktuelles Notfallkonzept vorhanden und greifbar?
- Kennen die Mitarbeiter das Notfallkonzept?
- Werden die definierten Rollen von den Mitarbeitern eingenommen, d. h. wissen die Mitarbeiter, was zu tun ist (Eskalationsstufen) und wen sie informieren müssen (Telefon- und Fax-Nr., Email-Adressen)?
- Sind die Mittel für den Workaround verfügbar, wie Handys, Faxgeräte, Telefonlisten, Notebooks, Büromaterial, Formulare, Checklisten, etc.
- Feststellung der Anzahl von Geschäftsvorfällen in der Zeit der Notfallübung. Gibt es hier Kriterien dafür, dass nur wichtige Geschäftsvorfälle bearbeitet oder priorisiert wurden?
- Werden Informationen, Dokumente zeitnah weitergereicht (per Telefon, Email, Fax) und von der empfangenden Stelle direkt weiterbearbeitet?
- Funktioniert der Wiederanlauf zum Ende der Notfallübung einwandfrei (Doppelbuchung, manuelle Nachpflege, etc.)?
- Anhand der Messgrößen ist auch festzulegen, unter welchen Umständen und bei Erreichung welcher Zielgrößen der Notfalltest erfolgreich ist.

Es sind Ausstiegspunkte vorzusehen, zu denen die Notfallübung abgebrochen werden kann. Hierzu sind auch Kriterien festzulegen, unter denen der Abbruch der Übung eingeleitet wird.

Nun wird der Ablauf der Notfallübung beschrieben. Dabei ist vor dem Start der Notfallübungen festzulegen, welche organisatorischen oder technischen Maßnahmen durchzuführen sind, die den Notfall simulieren (Berechtigungen sperren, Systeme herunterfahren, Strom abschalten, Arbeitsplatz sperren, Telefon außer Betrieb nehmen, etc).

Nun kann überlegt werden, ob die Mitarbeiter anhand der Umstände den Notfall erkennen oder ob seitens des NF-Managers die Notfallübung ausgerufen wird. Aus dieser Sachlage heraus sind dann die Prozesse der Eskalation wichtig, d. h.

wann wird der UHD und der Anwendungs- und Systembetreuer zwecks Fehlerlokalisierung informiert und wann erhalten die entsprechenden Führungskräfte eine Mitteilung. Nach Ablauf einer vorgegebenen Zeitspanne muss seitens der verantwortlichen Führungskraft der Notfallplan in Kraft gesetzt und der Krisenstab informiert werden. Während die Mitarbeiter nach dem Notfallplan arbeiten, ist es wichtig, die entsprechenden Kontroll- und Messgrößen zu erheben und den Ablauf zu beobachten. Ergänzend kann auch die Kommunikation und Zusammenarbeit zwischen dem FB und den Serviceeinheiten oder Dienstleistern, die die Fehler lokalisieren, beheben und den Wiederanlauf organisieren, zur Überprüfung in das Drehbuch aufgenommen werden.

Nach Ablauf der geplanten Notfallübungszeit wird der Wiederanlauf gestartet und es findet der Übergang in den standardmäßigen Prozessablauf statt. Hier muss nun sichergestellt werden, dass die Anwendungen, Systeme, Infrastrukturen, etc. wieder verfügbar sind und dass die Datenkonsistenz hergestellt und überprüft wird (Doppel-, Fehlbuchungen). Ebenfalls ist seitens der Führungskräfte der Notfall als beendet zu erklären und der Krisenstab aufzulösen.

Bei der Erstellung des Drehbuchs ist es wichtig, dass die Risiken, die bei der Durchführung einer Notfallübung entstehen, identifiziert und analysiert werden. Zur Minimierung von Risiken sind entsprechende Vorkehrungen zu treffen sowie mögliche Zeitpunkte des kontrollierten Abbruchs und Wiederanlaufs vorzusehen.

Aufgrund der sehr unterschiedlichen Rahmenbedingungen und Anforderungen an ein Drehbuch ist ein allgemeingültiges Template als Vorgabe nicht möglich, als Anhaltspunkt kann aber folgende Struktur genommen werden:

- Vorbereitende Maßnahmen vor der Übung;
- Start der Notfallübung;
- Simulation der Notfallsituation;
- Identifizierung der Notfallsituation seitens des FB;
- Information an UHD und Initiierung der Fehlerlokalisierung, Fehlerbehebung;
- Information der unmittelbaren Vorgesetzten;
- Inkraftsetzung und Durchführung des Notfallplans, Workaround;
- Einberufung des operativen Krisenstabs;
- Wiederanlauf;
- Beendigung der Notfallsituation;
- Nacherfassung und Sicherstellung der Datenkonsistenz;
- Nachbereitung (Manöverkritik, Schwachstellen, Verbesserungsmaßnahmen).

Zum effizienten Ablauf sind für die kritischen Passagen des Drehbuchs so weit wie möglich Checklisten, eindeutige Anweisungen und konkrete Zeiten vorzugeben.

Das Drehbuch ist nach Fertigstellung mit den Entscheidungsträgern abzustimmen, wobei die Ankündigung, der Verlauf, die einzelnen Ereignisse und Zeitpunkte, die Messgrößen sowie die beteiligten Personen festgelegt werden. Ebenfalls sind auch die Risiken zu betrachten und Absprachen zu treffen, unter welchen Bedingungen die Notfallübung vorzeitig beendet wird.

Nach der Fertigstellung des Drehbuchs ist bei komplexen Notfallübungen eine Trockenübung (Generalprobe) im kleinen, fachlich kundigen Kreis empfehlenswert, um die Abläufe in ihrer Logik zu überprüfen.

Durchführung der Notfallübung

Die Notfallübung wird termingerecht und nach den Vorgaben des Drehbuchs durchgeführt (siehe Abb. 30). Sollten sich während der Übung Probleme einstellen, so dass sich aus der Fortführung nicht mehr steuerbare und nicht mehr kalkulierbare Risiken ergeben, so ist die Übung sofort einzustellen und der Wiederanlauf durchzuführen.

Nach jeder Notfallübung sind die Ergebnisse entsprechend auszuwerten und in einem Ergebnisprotokoll zu dokumentieren.

Ergebnisprotokoll Notfallübung

Nach Ende einer Notfallübung ist zwingend ein Ergebnisprotokoll zu erstellen, in dem die Messgrößen und die Ergebnisse aufgeführt werden. Als Leitfaden kann das folgende Beispiel für ein Protokoll genutzt werden. Darüber hinaus können weitere aussagekräftige Punkte aufgenommen werden.

Ergebnisprotokoll:

- Bewerten Sie die Reaktion des Fachbereichs, als dieser erfuhr, dass ein kritisches System/Plattform/Anwendung ausgefallen oder teilweise ausgefallen ist;
- Wie wurde die erkannte Notsituation im FB kommuniziert?

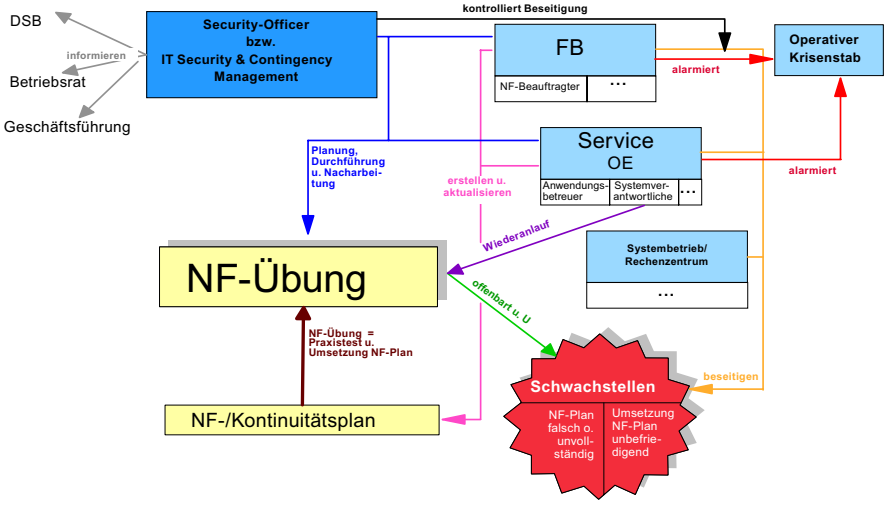


Abb. 30 Funktionen und Zuständigkeiten innerhalb einer Notfallübung

- Anhand welcher Kriterien wurde der Notfall identifiziert?
- Wer alarmierte den Krisenstab, bzw. bekam der Krisenstab Kenntnis vom Notfall?
- Wann trat der operative Krisenstab zusammen?
- Wurde der Notfall ordnungsgemäß, nach Überschreitung des kritischen Zeitraums (siehe Notfallplan), ausgerufen?
- War der Übergang von dem normalen Geschäftsablauf zum Anlauf der Notfall- und Kontinuitätspläne zügig, unproblematisch und effektiv?
- Waren dokumentierte Notfallpläne im Fachbereich vorhanden, vollständig, aktuell und für das betroffene Personal auffindbar?
- War das Szenario mit den Notfall- und Kontinuitätsplänen zu bewältigen und wenn ja, wurde den Vorgaben des Plans gefolgt?
- Waren die Notfall- und Kontinuitätspläne verständlich und waren die Mitarbeiter im Umgang mit den Plänen vertraut?
- Waren die zur Durchführung der Notfall- und Kontinuitätspläne erforderlichen Mittel in ausreichendem Maße vorhanden (Formulare, Checklisten, Handys, Büromaterial, …)?
- Wie war die fachbereichsinterne Kommunikation während der Umsetzung des Plans?
- Wie war die fachbereichsexterne Kommunikation: fristgerecht, effektiv, …?
- Wurden übergeordnete Aufgaben abgestimmt?
  - Zu anderen betroffenen FBen?
  - Zur nächst übergeordneten OE (Management, …)?
  - Zu Kunden?
- Konnte festgestellt werden, welche Geschäftsvorgänge abgeschlossen und welche noch offen waren?
- Lag eine aktuelle Datensicherung vor, wann war diese verfügbar?
- Gab es laut Plan eine verantwortliche Person für die Notfallsituation und einen Vertreter? War mindestens eine dieser Personen erreichbar?
- Kam gemäß Plan klar zum Ausdruck,
  - wer die kritischen Geschäftspartner sind und wann und wie diese zu informieren sind?
  - Wo die Schnittstellen des Geschäftsprozesses sind, was an diesen passiert und wer die Ansprechpartner sind?
  - Wer für den Wiederanlauf zuständig ist?
- Waren den Mitgliedern bzw. den Stellvertretern des FBs ihre zugeschriebenen Rollen, Kompetenzen und Verantwortungen klar?
- War die Informationsweitergabe bzgl. anderer betroffener Geschäftsprozesse fristgerecht und erfolgreich?
- Unterstützte der Plan ausreichend die geforderten Prozesse?
- Gab es ein Verfahren zur Wiederherstellung verlorener oder beschädigter Daten?

- Gab es Verfahren, um vom Notfallbetrieb zum normalen Geschäftsbetrieb zurückzukehren, inklusive der Konsistenz der Daten (Wiederanlauf)? Konnte der Wiederanlauf ordnungsgemäß durchgeführt werden?
- Anhand welcher Kriterien wurde das Ende der Notsituation identifiziert? Ist das Ende des Notfalls erklärt worden? Wurden die Geschäftspartner/Kunden über den Normalzustand informiert?
- Konnte die Ursache für das Eintreten der Notfallsituation ausfindig gemacht werden und wurden Maßnahmen für die zukünftige Vermeidung eingeleitet?

Abgleich der Sollwerte mit den Istwerten; gab es hier Abweichungen? Ist die Überarbeitung der Notfallpläne notwendig? Maßnahmenkatalog mit Verantwortlichen für die Umsetzung der Maßnahmen und Zeitvorgabe festlegen. Ist die bisherige Einschätzung des IT-Risikos für den Prozess/die Anwendung noch richtig oder sind Anpassungen notwendig?

8.2.7 K-Fall-Übungen

Szenarien

Es sind mindestens folgende Szenarien für einen K-Fall in Betracht zu ziehen:

- Brand;
- Wassereinbruch;
- Stromausfall;
- Ausfall der Klimaanlage;
- Explosion;
- Flugzeugabsturz;
- Geiselnahme;
- Ausfall der Datenübertragung;
- Ausfall des Rechenzentrums;
- Sabotage;
- Gefahreneinwirkung von außen;
- Bombenalarm;
- Umgestürzter LKW mit Gefahrgut (schwer, aufwendig zu beseitigen, Explosionsgefahr);
- Verstrahlung, Kontamination;
- Pandemie.

Überblick zu Planung, Durchführung, Nachbereitung von K-Fall-Übungen

Die Steuerung und Initiierung von K-Fall-Übungen obliegt dem Security-Officer, bzw. einem IT-Security & Contingency Management, das Vorschläge für eine K-Fall-Übung auf Basis der aufgeführten Szenarien sowie Standort, Flächen,

Gebäudeteile oder sogar Gebäude unterbreitet. Termine für die Durchführung der K-Fall-Übung werden mit den beteiligten FB abgestimmt. In Abstimmung mit Vorstand, Verwaltung, Revision und den tangierten Bereichsleitern wird die Durchführung der K-Fall-Übung beschlossen.

Bei der Planung und Durchführung einer K-Fall-Übung sind folgende Schritte durchzuführen:

- Festlegung des K-Fall-Szenarios;
- Zusammenstellung einer Namensliste mit den Personen, die im Vorfeld informiert und einbezogen werden;
- Festlegen von Ort, Start, Ende, Simulationszeitraum der K-Fall-Übung;
- Festlegung der Wirkung des K-Fall-Szenarios auf Ort, Fläche, Personen, etc.;
- Ist die Simulation des K-Falls über mehrere Tage als Zeitraffer zu berücksichtigen?
- Überprüfung, welche Systeme und Anwendungen betroffen sind;
- Prüfung der Präventivmaßnahmen;
- Festlegung weiterer Sicherungsmaßnahmen, Verfügbarkeiten, Rufbereitschaften vor der K-Fall-Übung;
- Verfahren des Wiederanlaufs zum Normalbetrieb festsetzen;
- Definition des Monitorings während der K-Fall-Übung;
- Besetzung der steuernden und stützenden Rollen während der K-Fall-Übung;
- Aufzeigen der Risiken durch die K-Fall-Übung.

Nachdem die Rahmenbedingungen für den K-Fall-Test feststehen, ist ein Drehbuch zu erstellen, das den Ablauf beschreibt. In einer letzten Abstimmungsrunde wird das Drehbuch von den tangierten Bereichsleitern verabschiedet. Dann wird eine Vorstandsvorlage erstellt und dem Vorstand zur Zustimmung vorgelegt.

Die K-Fall-Übung wird anhand des Drehbuchs durchgeführt. Direkt im Anschluss wird eine Gesprächsrunde für eine Manöverkritik durchgeführt und wichtige Erkenntnisse werden protokolliert.

Der Security-Officer bzw. das IT-Security & Contingency Management wertet die Ergebnisse aus und erstellt einen Bericht über die K-Fall-Übung. Der Bericht enthält Informationen über die erfolgreichen Passagen und Schwachstellen der K-Fall-Übung sowie einen Maßnahmenkatalog mit Empfehlungen von Verbesserungsmaßnahmen (mit Sofortmaßnahmen). Anhand der Auswertung erfolgen gegebenenfalls Anpassungen der Präventivmaßnahmen und eine Überarbeitung der Notfallpläne. Im Nachgang wird, sofern bestimmbar, eine hypothetische Schadensermittlung durchgeführt.

Die Umsetzung der Sofortmaßnahmen und Beseitigung von Schwachstellen obliegt den jeweils tangierten und verantwortlichen FB.

Abstufungen von K-Fall-Übungen

Um einen geordneten Ablauf sicherzustellen und die Mitarbeiter, die an der K-Fall-Übung teilnehmen, nicht zu überfordern, ist es sinnvoll, diese mit jeder

Übung näher an die Realität heranzuführen. Der Schwierigkeitsgrad der K-Fall-Übung wird von Übung zu Übung wie folgt gesteigert:

- Stufe 1: Die tangierten Mitarbeiter werden ca. vier Wochen vorher über die Durchführung einer K-Fall-Übung informiert, wobei der Termin mit Uhrzeit bekannt gegeben wird. Es finden im Vorfeld Besprechungen, Abstimmungen und Schulungen zur Sensibilisierung statt; das Vorhandensein und die Funktionsfähigkeit der Präventivmaßnahmen werden geprüft.
- Stufe 2: Die tangierten Mitarbeiter werden ca. eine Woche vorher informiert, an welchem Tag die K-Fall-Übung stattfindet. Es findet kein Training, keine Sensibilisierung und keine Überprüfung der Präventivmaßnahmen statt.
- Stufe 3: Die Mitarbeiter werden unmittelbar vorher (eine Stunde) informiert.
- Stufe 4: Die K-Fall-Übung wird ohne vorherige Information und Ankündigung gestartet.

Die Festlegung der Stufe für die Durchführung der K-Fall-Übung wird als Empfehlung vom Security-Officer bzw. vom IT-Security & Contingency Management in den Vorschlag der K-Fall-Übung eingearbeitet.

Häufigkeit und Anforderungen an eine K-Fall-Übung

K-Fall-Übungen werden vom Security-Officer bzw. von einem installierten IT-Security & Contingency-Management initiiert und durchgeführt. Pro Jahr ist mindestens eine K-Fall-Übung zu planen und durchzuführen. Für die Durchführung von K-Fall-Übungen sind wie bei der Notfallübung Prüfkonzepte zu entwickeln und Messgrößen vorzugeben, über die dann im Rahmen der Übung das Ineinandergreifen der verschiedenen Notfall- und Kontinuitätspläne nachgewiesen werden kann. K-Fall-Übungen sind im laufenden Geschäftsbetrieb und an produktiven Systemen durchzuführen.

Checkliste für die Planung einer K-Fall-Übung

Die K-Fall-Übung geht von einem Katastrophenszenario aus. Hier gilt es zunächst den Umfang und die Wirkung eines solchen Szenarios zu eruieren und zu überprüfen, welche der Notfallpläne in diesem komplexen Zusammenhang greifen. Im Folgenden ist ein Template (siehe Tabelle 39), das für eine geplante K-Fall-Übung entsprechend genutzt und angepasst werden kann.

Tabelle 39 Checkliste „Planung einer K-Fall-Übung“

1	Protokollant:	Name: OE:
2	Datum und Uhrzeit der angesetzten K-Fall-Übung:	Datum: tt.mm.jj Von: *hh:mm* Bis: *hh:mm*
3	Leiter der K-Fall-Übung	Name: *(z. B. Security-Officer)*

Tabelle 39 (Fortsetzung)

4	Festlegen des K-Fall-Szenarios:	Brand, Geiselnahme, Sabotage, Stromausfall, Flugzeugabsturz, …
5	Ort der Einwirkung des Szenarios:	Lokation, Gebäude, Etage, Infrastruktur, DV-Systeme, Prozesse/IT-Anwendungen?
6	Betroffene OEen:	• Welche Mitarbeiter nehmen an der Übung teil? • Welche Prozesse, Anwendungen, Systeme und Plattformen sind betroffen? • Ist RZ oder ext. Dienstleister mit einzubinden?
7	Erstellung eines Drehbuchs:	Vorgehensweise innerhalb der Übung, Rollen- und Aufgabenverteilung, Verantwortlichkeiten festlegen, Start-, Endetermin, Zeitraffer, Checkpoints, Wiederanlauf, Dokumentation, Nacharbeiten und Qualitätscheck, etc.
8	Ziele bzw. erwartete Ergebnisse:	Aufzeigen der messbaren, nachprüfbaren Ergebnisse, die den Erfolg der Übung widerspiegeln.
9	Risiken der Übung:	Aufzeigen möglicher Gefahren und Risiken, die aus der Initiierung und Durchführung der Übung selbst resultieren. Systeme wirklich abschalten? Raum ist für mehrere Stunden nicht mehr betretbar?
10	Abstimmung mit den OEen erfolgt? Vorangekündigte Übung?	• Stufe 1: Vier Wochen vorher mit Termin und Uhrzeit (Urlaubssperre?); • Stufe 2: Eine Woche vorher mit Angabe des Tages (Urlaubssperre?); • Stufe 3: Eine Stunde vorher; • Stufe 4: Ohne Vorankündigung.
11	Art der Übung:	□ Schreibtisch-Übung/Workshop □ Praktische Übung vor Ort □ Sonstige
12	Räumlichkeiten:	Lokation, Gebäude, Etage, Raum festlegen
13	Notwendige Ausrüstung:	□ Overhead □ Flipchard □ Moderatorenkoffer □ Pinnwand □ Beamer
14	Notwendige Personen (Namen, OE, Funktion)	NF-Manager: OE: Tel.: Vertreter: Mitarbeiter aus FB: OE: Tel.: Vertreter: Anwendungsbetreuer: OE: Tel.: Vertreter: Systembetreuer: OE: Tel.: Vertreter: Verwaltung/Facilitymanagement: OE: Tel.: Vertreter:
	Operativer Krisenstab:	Name: OE: Tel.: Vertreter: Name: OE: Tel.: Vertreter:
	Strategischer Krisenstab:	Name: OE: Tel.: Vertreter: Name: OE: Tel.: Vertreter:

Tabelle 39 (Fortsetzung)

15	Zeitrahmen der K-Fall-Übung:	Beginn: Ende: (Welcher Zeitraum soll simuliert werden, z. B. 5 Tage; wie sehen die Steps der Zeitraffung aus, wie können diese zeitlich simuliert werden?)
16	Wiederanlauf:	Name: OE: Tel.: (notwendige und verantwortliche Personen)
17	Bemerkungen:	

Anmerkung: Bitte Tabelle ergänzen und ausfüllen

Erstellung eines Drehbuchs für eine K-Fall-Übung

Generell ist bei der Gestaltung des K-Fall-Drehbuchs eine Analogie zur Erstellung eines Drehbuchs für eine Notfallübung zu sehen, wobei eine K-Fall-Übung eine wesentlich komplexere Art von Notfall-Übung ist und mehrere Notfallpläne gleichzeitig greifen. Als Beispiele sind hier folgende Szenarien zu nennen:

- Brand eines Gebäudeteils, eines Gebäudes, in dem wichtige Geschäftsprozesse ablaufen (z. B. Handelsräume bei einem Finanzinstitut). Durch die Katastropheneinwirkung sind mehrere unternehmensnotwendige Geschäftsprozesse bzw. Anwendungen sehr stark eingeschränkt oder überhaupt nicht mehr verfügbar.
- Geiselnahme im Vorstandsbereich; hier kann mit der kompletten Räumung des Gebäudes gerechnet werden; die Geschäftstätigkeit kann gravierend gestört werden.
- Bombenanschlag auf einen Gebäudeteil; situativ kann der Geschäftsbetrieb erheblich beeinträchtigt werden.
- Hackerangriff, Sabotage; situativ erhebliches Gefahrenpotenzial, weil die Geschäftsprozesse nicht mehr sicher steuerbar sind und die Datenkonsistenz unsicher ist.

Für das K-Fall-Drehbuch ist primär das IT-Security & Contingency Management zuständig. Anhand des K-Fall-Szenarios sind die tangierten OEen und deren betroffene Geschäftsprozesse/Anwendungen zu identifizieren (siehe Abb. 31) Auf dieser Basis sind die einzelnen Drehbücher durch die zuständigen Notfallmanager der jeweiligen FB zu erstellen. Das IT-Security & Contingency Management koordiniert die Zusammenführung der einzelnen Drehbücher in ein Gesamtwerk. Hier sollten auch Checkpoints und Ausstiegspunkte für den Abbruch der K-Fall-Übung mit eingearbeitet werden.

Das Drehbuch ist nach Fertigstellung als Entscheidungsvorlage dem Vorstand vorzulegen und zu genehmigen, wobei insbesondere auch auf die Risiken, die durch die K-Fall-Übung entstehen, hingewiesen wird.

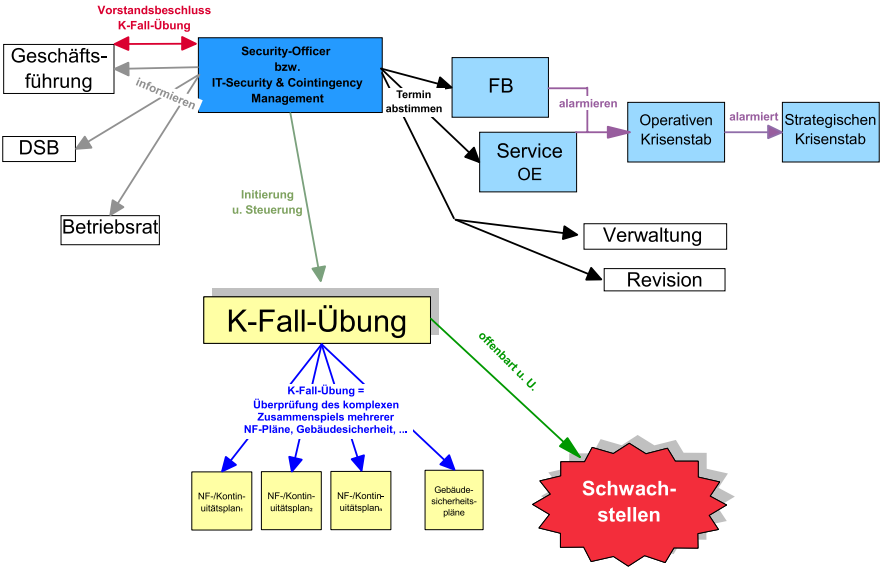


Abb. 31 Funktionen und Zuständigkeiten bei einer K-Fall-Übung

Durchführung der K-Fall-Übung

Die K-Fall-Übung wird, nachdem der Vorstand diese genehmigt hat, termingerecht und nach den Vorgaben des Drehbuches durchgeführt. Während dieser Übung ist auch der strategische Krisenstab involviert. Sollten sich während der Übung Probleme einstellen, so dass sich aus der Fortführung nicht mehr steuerbare und nicht mehr kalkulierbare Risiken ergeben, so ist die Übung schnellstmöglich abzubrechen und der Wiederanlauf des Normalbetriebs unverzüglich einzuleiten.

Nach jeder K-Fall-Übung sind die Ergebnisse entsprechend auszuwerten und in einem Ergebnisprotokoll zu dokumentieren.

Ergebnisprotokoll K-Fall-Übungen

Als Muster kann das Ergebnisprotokoll der Notfall-Planung genutzt werden. Zusätzlich sind folgende Fragen zu betrachten, wobei individuell weitere Punkte aufgenommen werden können.

Ergebnisprotokoll:

- War das Szenario der K-Fall-Übung zu bewältigen und steuerbar und wenn ja, wurde den Vorgaben des Plans gefolgt?
- Waren die Moderation und das Coaching während der K-Fall-Übung durch den Security-Officer bzw. durch das IT-Security & Contingency-Management und die Notfallmanager hilfreich und zielführend?

- Wie war in dem komplexen Umfeld die Kommunikation während der K-Fall-Übung:
  - zu Kunden?
  - zwischen den betroffenen Fachbereichen?
  - zu Dienstleistern (Rechenzentrum, externe Dienstleister, Infodienste)?
  - zum operationalen und strategischen Krisenstab? Wurden übergeordnete Aufgaben abgestimmt und priorisiert?
- War das Zusammenwirken aller in Kraft gesetzten Notfall- und Kontinuitätspläne unproblematisch und effektiv?
- Hat der operative und strategische Krisenstab seine Aufgabe wahrgenommen?
- Ableitung eines Maßnahmenkataloges aus erkannten Schwachstellen.

Festlegung, durch wen und bis wann unverzügliche Maßnahmen umzusetzen sind. Ebenfalls ist festzuhalten, wie mit den weiteren Schwachstellen verfahren wird und welche abgestellt werden.

Kontrollinstanzen und Berichtswege für die Umsetzungsmaßnahmen klarstellen. Die Zuständigkeiten können je nach Aufbau- und Ablauforganisation beim zuständigen Fachbereich und deren Notfallmanager, bei Kompetenzcentern, bei den zuständigen Anwendungs- und Systembetreuern oder bei dem Security-Officer bzw. beim IT-Security & Contingency-Management liegen. Kontrollinstanzen sollten unabhängig sein. Bei kleineren Maßnahmen können die Ergebnisse oder der Fortschritt z. B. an den Security-Officer bzw. an das IT-Security & Contingency-Management berichtet werden, bei größeren Umsetzungsmaßnahmen können die Aktivitäten in die normale Projektarbeit integriert werden, wobei hier an einen Lenkungsausschuss oder ein ähnliches Gremium berichtet wird.

Anhang

A.1 Begriffsdefinitionen Sicherheit

Im Folgenden werden die Grundbegriffe der Sicherheit kurz erläutert.

Sicherheit Der Begriff Sicherheit umschreibt die wissenschaftliche, technologische und ingenieurmäßige Behandlung von Sicherheitsaspekten zur Schadensvermeidung oder bei Sicherheitsverletzungen zur Schadensbegrenzung.

IT-Sicherheit Unter dem Begriff IT-Sicherheit wird die wissenschaftliche, technologische und ingenieurmäßige Behandlung von Sicherheitsaspekten in der Informationstechnologie verstanden. Diese beinhaltet insbesondere die Aspekte der Informationssicherheit, d. h. den Schutz von Informationen im Hinblick auf Vertraulichkeit, Integrität, Verfügbarkeit, Verbindlichkeit und Authentizität.

Vertraulichkeit Vertraulichkeit bedeutet, dass eine Kenntnisnahme von Informationen ausschließlich durch dazu berechtigte Personen erfolgt.

Integrität Unter Integrität wird die physische und logische Unversehrtheit von Systemen, Anwendungen und Daten verstanden. Dies beinhaltet auch, dass Informationen nur von dazu Berechtigten in jeweils zulässiger Weise geändert werden können.

Verfügbarkeit Verfügbarkeit bedeutet, dass benötigte Daten innerhalb einer akzeptablen Zeitspanne zur Verfügung stehen.

Verbindlichkeit Verbindlichkeit bedeutet, dass Sender und Empfänger von Daten zweifelsfrei nachgewiesen werden können. Zur Verbindlichkeit gehören auch die Aspekte Nichtabstreitbarkeit, Beweissicherheit, Nachweisbarkeit, Verantwortlichkeit.

Authentizität Unter Authentizität wird die Echtheit, Zuverlässigkeit und Glaubwürdigkeit der Kommunikationspartner bzw. deren Mitteilungen verstanden. Sie ist in vielen Fällen nach heutiger Rechtsauffassung nur bei originaler Mitteilung z. B. bei Direktkommunikation, als Schriftgut mit originaler Unterschrift der zur Abgabe von schriftlichen Willenserklärungen autorisierten Personen oder bei Verwendung einer digitalen Signatur gem. Signaturgesetz gewährleistet. In einigen Fällen schreibt das Gesetz zur Sicherung der Authentizität notarielle Beglaubigung oder Beurkundung vor.

Störfall Ein Störfall ist ein Zustand, der infolge eines überraschenden und außerordentlichen Ereignisses entsteht, wobei dieser Zustand mit vorhandenen Mitteln im Rahmen der bestehenden Aufbau- und Ablauforganisation bewältigt werden kann.

Katastrophe, Notfall Ein Katastrophen- (K-Fall) oder Notfall ist ein Zustand, der infolge eines überraschenden und außerordentlichen Ereignisses eintritt und dessen Auswirkungen nicht mit den vorhandenen Mitteln der bestehenden Aufbau- und Ablauforganisation bewältigt werden kann. Ein Notfall liegt vor, wenn ein oder wenige Prozesse des Geschäftsbetriebs nicht in der notwendigen Weise verfügbar sind, sodass eine substantielle Existenzgefährdung des Unternehmens entstehen kann. Ein K-Fall liegt vor, wenn ein extern nicht beeinflussbares Ereignis (Wasser, Brand, Explosion, Geiselnahme, etc.) auf das Unternehmen so einwirkt, dass eine substantielle Existenzgefährdung (z. B. Standort ist nicht verfügbar) entstehen kann.

A.2 Checkliste: Organisation der IT-Sicherheit

Kriterien	Status
Ist in allen Unternehmensbereichen die Rolle der IT und insbesondere der IT-Sicherheit bekannt?	
Welche Kosten entstehen, wenn ein wichtiger Produktions-Server 1–4 Std., ½ oder 1 Tag, eine Woche ausfällt?	
Welche Zeit dauert die Wiederherstellung eines produktiven Systems (Rücksicherung Systeme, Daten); was für Kosten entstehen? Wer übernimmt die Kosten?	
Wie lange dauert es durchschnittlich, bis ein Sicherheitsproblem überhaupt festgestellt und behoben wird? • Allg. Hardware-, Softwareproblem • Virus, Trojaner • Hackerangriff, Phishing • Datenentwendung, Verfälschung, Sabotage • Datenverlust?	
Wird sichergestellt, dass sich ein bekanntes Sicherheitsproblem nicht wiederholt? Wenn ja, wie?	
Werden die Basis-Sicherheitssysteme wie Firewall und Virenscanner täglich aktualisiert?	
Gibt es im Unternehmen eine schriftliche und aktuelle Security Policy? • Unternehmens-Policy Sicherheit, IT-Sicherheit • Policy für E-Mail, Internet, Datenaustausch, etc. • Zugriffsrechte, Zugriffsschutz (RAS, WLAN) • Zutrittsregelung in sicherheitsrelevante Räume?	
Gibt es Regeln zur Privatnutzung von E-Mail und Internet?	
Sind die Zuständigkeiten und Verantwortlichkeiten in einer sicherheitsrelevanten Situation den Beteiligten bekannt?	
Haben alle Mitarbeiter bei Sicherheitsfragen einen direkten Ansprechpartner, bzw. Zugriff auf aktuelle Security-Unterlagen?	
Kenne ich die rechtlichen Anforderungen, die für mich und das Unternehmen relevant sind? • Geheimhaltungs-, Vertraulichkeitserklärung • Datenschutzgesetz • KonTraG, KWG, MaRisk, … • Haftung, Gewährleistung • Erfüllungen aus SLAs, Geschäftsbesorgungsvertrag?	
Sind alle sicherheitsrelevanten Systeme ausreichend dokumentiert?	
Wird das Thema IT-Sicherheit von der Unternehmensführung mit getragen?	
Wie hoch ist im Schadensfall der Imageverlust bei Partnern, Kunden und Lieferanten?	
Existiert für den Schadensfall ein Plan zur Information von Behörden, Mitarbeitern, Medien und Öffentlichkeit?	
Gibt es einen Notfallplan, Katastrophenplan? Übungen?	
Gibt es Kontinuitätsmaßnahmen für Kerngeschäftsprozesse?	
Gibt es ein Konzept, um einen wirksamen und gleichzeitig wirtschaftlich sinnvollen Schutz zu erreichen?	
Ist das Restrisiko angemessen versichert, verlagert?	

Anmerkung: Bitte Tabelle anpassen und ausfüllen

A.3 Checklisten für innere Sicherheit

Kriterien	Status
Sind die Server- und Verteilerräume verschlossen?	
Wird der Zugang zu kritischen Systemen und Räumen kontrolliert und protokolliert (personifizierter Zugang, Kameraüberwachung)?	
Sind die Zutrittsberechtigungen zu sicherheitskritischen Räumen schriftlich geregelt (und auch zeitlich begrenzt)?	
Werden Zutrittsmittel (Schlüssel, PIN für elektronische Zugangssicherung) sicher verwaltet (Tresor, eigener Sicherheitsbereich)?	
Ist der Zugang externer Mitarbeiter (Wartungs- und Reinigungspersonal, Handwerker) gesondert geregelt?	
Sind Maßnahmen bei Eintritt, Austritt, Versetzung, Beförderung von Mitarbeitern eindeutig geregelt (Laufzettel der Personalabteilung)?	
Werden die Arbeitsplätze der Mitarbeiter regelmäßig auf Spyware und Trojaner untersucht?	
Sind die Sicherheitseinstellungen auf den Clients (Zugriff, Browser, Makros) schriftlich definiert und den Mitarbeitern bekannt?	
Wird die Vergabe von Benutzerrechten eindeutig reguliert?	
Wird eine starke Benutzerauthentisierung verwendet?	
Sind die Vorgaben zur Verwendung von Passwörtern schriftlich fixiert und den Mitarbeitern bekannt (IT-Security-Policy)?	
Gibt es Kontrollmechanismen bei der Vergabe von Benutzerrechten (wer unterschreibt, wer genehmigt, wer kontrolliert Zugriff)?	
Werden die Passwörter regelmäßig geändert?	
Werden Accounts bei fehlerhaften Anmeldungsversuchen gesperrt?	
Werden Logfiles auf gescheiterte Anmeldeversuche überprüft?	

Anmerkung: Bitte Tabelle anpassen und ausfüllen

A.4 Checklisten für äußere Sicherheit

Kriterien	Status
Ist eine Firewall installiert (Hard- oder Software; Aktualisierung)?	
Ist sichergestellt, dass die Firewall richtig konfiguriert ist und eine regelmäßige Aktualisierung stattfindet (stündlich, täglich)?	
Werden Protokolldateien und Konfiguration der Firewall regelmäßig überprüft?	
Sind die für den externen Zugang notwendigen Server in einer DMZ aufgestellt?	
Sind alle Server in der DMZ mit allen aktuellen Sicherheits-Updates ausgestattet?	
Wird Virenscanner bei Up- oder Download von Daten aus dem Internet eingesetzt?	
Wird ein Virenscanner eingesetzt, der ein- und ausgehende E-Mails überprüft?	
Wird der Scanner täglich aktualisiert?	
Sind aktuelle Spam-Filter im Einsatz?	
Werden Protokolldateien und Konfiguration der Virenscanner regelmäßig überprüft?	

Anmerkung: Bitte Tabelle anpassen und ausfüllen

A.5 Checkliste Mitarbeiter

Kriterien	Status
Wird bei der Auswahl und beim Einsatz der Mitarbeiter auf Vertrauenswürdigkeit geachtet? (Externe Mitarbeiter in sicherheitsrelevanten Bereichen, dann polizeiliches Führungszeugnis, Referenzen?)	
Werden die Mitarbeiter im Arbeitsvertrag auf die IT-Sicherheit und das Datenschutzgesetz verpflichtet?	
Ist den Mitarbeitern die Sicherheitsleitlinie bekannt und erläutert worden? (Wann, von wem, Protokoll und Unterschrift?)	
Sind den Mitarbeitern die Ansprechpartner für IT-Sicherheitsthemen bekannt (Security-Officer, Compliance-Beauftragter, UHD)?	
Werden regelmäßig Schulungen zum Thema IT-Sicherheit durchgeführt? (Wie oft, von wem?)	
Erkennen Mitarbeiter typische Merkmale virenverseuchter E-Mails, Hackerangriffe oder sonstige Anormalitäten?	
Ist ausreichendes Informations- und Aufklärungsmaterial vorhanden und jedem Mitarbeiter leicht zugänglich?	
Welche Richtlinien und Vorgaben gelten für die Mitarbeiter? (E-Mail-, IT-Security-, Internet-Policy)	
Sind diese Richtlinien den Mitarbeitern bekannt? In welcher Form (Intranet, Papieranweisung)?	
Sind den Mitarbeitern die möglichen Sanktionen bei einem Verstoß gegen Richtlinien bewusst?	
Sind die Mitarbeiter über Notfallpläne und deren Inhalte informiert?	
Sind die Zugriffsrechte für jeden Mitarbeiter definiert?	

Anmerkung: Bitte Tabelle anpassen und ausfüllen

A.6 Checkliste Datensicherung

Kriterien	Status
Gibt es ein detailliertes Datensicherungskonzept (für eigene geschäftsrelevante E-Mails, Daten und Dokumente)?	
Existiert eine schriftliche, aktuelle Dokumentation?	
Sind die Zuständigkeiten und Verantwortlichkeiten allen Beteiligten bekannt und bewusst (auch Stellvertreter)?	
Sind die Aufbewahrungsorte der Sicherungskopien für die Lagerung geeignet?	
Sind die Sicherungskopien vor dem Zugriff Unbefugter geschützt?	
Werden die Logdateien der Datensicherung regelmäßig überprüft (Overflow)?	
Wird die Wiederherstellung der Daten regelmäßig geübt und protokolliert (Recovery-Maßnahmen, Backup einspielen)?	
Wird regelmäßig (z. B. jährlich) geprüft, ob die Sicherungsmedien noch lesbar sind?	
Existiert ein Konzept für die Langzeit-Archivierung?	
Sind hochverfügbare Server-RAID-Systeme im Einsatz? Werden diese auch geprüft?	

Anmerkung: Bitte Tabelle anpassen und ausfüllen

A.7 Checkliste Risikoanalyse und Sicherheitsziele

Kriterien	Status
Sind alle Kern-Prozesse im Unternehmen mit den jeweiligen IT-Verantwortlichen bekannt?	
Sind alle Vermögenswerte bekannt und bewertet (Hardware, Software, Daten, immaterielle)?	
Sind die Vermögenswerte und Prozesse dokumentiert?	
Sind mögliche Bedrohungen hinsichtlich Schadenshöhe und Wahrscheinlichkeit bekannt?	
Gibt es Risiko-Bewertungen und Einschätzungen über mögliche Schäden, die beim Verlust von Verfügbarkeit, Integrität oder Vertraulichkeit für das Unternehmen entstehen können?	
Sind Maßnahmen definiert, die mögliche Schäden auf ein wirtschaftlich tragbares Maß begrenzen? • Präventiv • Reaktiv	
Gibt es ein Verfahren, über das Veränderungen hinsichtlich Bedrohungen, neuen Umgebungen oder neuen Prozessen und IT-Systemen erfasst und bewertet werden (Steuerung operationaler Risiken)?	
Sind Abläufe und Verantwortlichkeiten für die laufende Risikobewertung definiert?	
Gibt es standardisierte Mitteilungen, Pressetexte an Benutzer, Kunden, Bevölkerung?	

Anmerkung: Bitte Tabelle anpassen und ausfüllen

A.8 Mustervorlage E-Mail-Richtlinien

I. Gegenstand und Geltungsbereich

Diese Richtlinie regelt die Grundsätze für die Nutzung der E-Mail-Dienste innerhalb der Firma mit allen Unternehmensbereichen und gilt für alle Beschäftigten, deren Arbeitsplätze über einen E-Mail-Zugang verfügen.

E-Mails werden beim Eintreffen bzw. vor dem Senden an zentraler Stelle und durch den Nutzer unbemerkt auf Viren und anderen schädlichen Code überprüft. Bei Heimarbeitsplätzen und Mobilgeräten ist durch den Nutzer sicherzustellen, dass sowohl eingehende als auch ausgehende E-Mails auf schädlichen Code überprüft werden, soweit dies nicht vom Benutzerservice schon fest eingestellt ist.

Bei geschäftsrelevanten E-Mails sind die notwendigen Geschäftsdaten, die gesetzlich für einen ordentlichen Geschäftsbrief gefordert werden, immer als Fußnoten anzufügen. Hier sollten auch aufgrund von Änderungen der Rechtsprechung regelmäßige Überprüfungen und Anpassungen vorgenommen werden.

Jede E-Mail, die das Unternehmen verlässt, muss eine Haftungsausschlusserklärung beinhalten. Der Wortlaut ist:

Diese E-Mail, einschließlich sämtlicher mit ihr übertragenen Dateien, könnte vertrauliche und/oder rechtlich geschützte Informationen enthalten. Wenn Sie nicht der richtige Adressat sind oder diese E-Mail irrtümlich erhalten haben, informieren Sie bitte sofort den Absender und vernichten Sie diese Mail. Das unerlaubte Kopieren sowie die unbefugte Weitergabe dieser Mail sind nicht gestattet.

This e-mail may contain confidential and/or privileged information. If you are not the intended recipient (or have received this e-mail in error) please notify the sender immediately and destroy this e-mail. Any unauthorised copying, disclosure or distribution of the material in this e-mail is strictly forbidden.

Ebenfalls sind alle gesetzlich geforderten Angaben zum Unternehmen bei einer Geschäfts-E-Mail wie bei einem normalen Geschäftsbrief mit anzugeben.

II. Verhaltensgrundsätze

Die Benutzung des E-Mail-Systems für private Zwecke ist nicht erlaubt.

Unzulässig ist das Versenden oder Verteilen von Material, wenn es gegen Gesetze oder gegen die guten Sitten verstößt, bzw. von anderen Personen als geschmacklos, Anstoß erregend oder respektlos angesehen werden könnte, wie z. B.

- Material, das sexuell eindeutige Bilder und Beschreibungen enthält;
- Material, das illegale Aktionen befürwortet;
- Material, das Intoleranz gegen Andere (z. B. Religion) befürwortet oder rassistischen Inhalt hat;
- Material, das Viren oder andere schädigende Software/Code enthält;
- E-Mails, die Spam sind oder die einen Kettenbrief oder Schneeballeffekt auslösen.

Jegliches Öffnen von nicht erwarteten und unbekannten E-Mails oder Dateianhängen ist nicht erlaubt. Es ist auch nicht gestattet, auf Werbung, Kettenbriefe etc. zu antworten oder diese weiterzuleiten. Ebenso darf nicht auf von außen kommende Virenwarnungen selbst durch eigene Maßnahmen reagiert werden. In all diesen Fällen ist unverzüglich die IT-Administration (User-Help-Desk) zu informieren.

Ebenfalls ist die IT-Administration unverzüglich zu informieren, wenn der Verdacht eines Virenbefall besteht oder sich das IT-System ungewöhnlich verhält. In dem Fall ist die Arbeit sofort einzustellen und es dürfen keine weiteren Mails und Anhänge mehr geöffnet werden.

III. Einwilligung und Vertretungsregelung

Durch die Nutzung des E-Mail-Dienstes erklärt der Beschäftigte seine Einwilligung in die Protokollierung und Kontrolle der Nutzung. Bei der Einrichtung einer Vertretungsregelung muss der Mitarbeiter den Zugang zu den E-Mails durch den Vertreter gewähren. Die Korrespondenz eines Mitarbeiters darf nicht ohne dessen Wissen eingesehen werden.

IV. Leistungs- und Verhaltenskontrolle/Datenschutz für E-Mail

Um Datendiebstahl und Missbrauch entgegenzuwirken, eventuelle Diskriminierung zu entdecken und den regulären Gebrauch zu überprüfen behält sich die Geschäftsführung vor, den E-Mail-Verkehr aufzuzeichnen. Soweit personenbezogene oder -beziehbare Daten aufgezeichnet werden, dürfen diese ausschließlich für die genannten Zwecke dieser Richtlinie verwendet werden. Daten über das Benutzerverhalten dürfen ausschließlich zur Gewährleistung der Systemsicherheit, zur Optimierung und Steuerung des Systems, zur Fehleranalyse und -korrektur sowie zur kostenstellenbezogenen Abrechnung der Systemkosten verwendet werden. Die Zugriffe auf diese Funktionen bleiben auf die mit der technischen Administration des Systems betrauten Personen begrenzt. Diese sind entsprechend auf Vertraulichkeit, Datenschutzgesetz und interne Betriebsvereinbarungen zu verpflichten.

Eine Verwendung der vorgenannten Daten zur weitergehenden Leistungs- oder Verhaltenskontrolle ist nicht gestattet. Bei einem ausreichend begründeten Verdacht kann mit Zustimmung des Betriebsrates die gezielte Überprüfung eines E-Mail-Accounts stattfinden. Bei der Überprüfung ist der betriebliche Datenschutzbeauftragte hinzuzuziehen. Maßnahmen, die den Missbrauch des E-Mail-Dienstes verhindern oder beweisen helfen, können bei Gefahr im Verzug (begründeter Verdacht) unmittelbar durchgeführt werden. In diesen Fällen sind der Datenschutzbeauftragte und anschließend der Betriebsrat unverzüglich zu informieren. Ein Verstoß kann neben den arbeitsrechtlichen Folgen auch strafrechtliche Konsequenzen haben. Die Geschäftsführung behält sich vor, bei Verstößen gegen diese Vereinbarung die Nutzung des E-Mail-Zugangs im Einzelfall zu untersagen.

Ort, Datum

Geschäftsführer/Betriebsrat

A.9 Übersicht von Normen für Zwecke des Notfall- und Kontinuitätsmanagements

- HGB: Handelsgesetzbuch
- AktG: Aktiengesetz
- PublG: Publizitätsgesetz
- GenG: Genossenschaftsgesetz
- KWG: Kreditwesengesetz
- VAG: Versicherungsaufsichtsgesetz
- SRVwV: Allgemeine Verwaltungsvorschrift über das Rechnungswesen in der Sozialversicherung
- SVRV: Sozialversicherungs-Rechnungsverordnung
- PharmBetrV: Betriebsverordnung für pharmazeutische Unternehmen
- KrW-/AbfG: Kreislaufwirtschafts- und Abfallgesetz
- NachwV: Nachweisverordnung
- AO: Abgabenordnung
- HGrG: Haushaltsgrundsätzegesetz
- BGB: Bürgerliches Gesetzbuch
- ZPO: Zivilprozessordnung
- StGB: Strafgesetzbuch
- UWG: Gesetz gegen den unlauteren Wettbewerb
- BetrVG: Betriebsverfassungsgesetz
- SigG: Signaturgesetz
- SigV: Signaturverordnung
- BDSG: Bundesdatenschutzgesetz
- BS: British Standard 25999

Gesetzessammlung: http://www.gesetze-im-internet.de

Abkürzungsverzeichnis

AktG	Aktiengesetz
AO	Abgabenordnung
Basel II	Richtlinien zum Absichern von Risiken (Kreditrisiken, operationale Risiken, …)
BDSG	Bundesdatenschutzgesetz
DB	im betriebswirtschaftlichen Kontext = Deckungsbeitrag im IT-Kontext = Datenbank
DIN	Deutsche Industrienorm
FB	Fachbereich, Abteilung
FMEA	Fehlermode and effect analysis
GoB	Grundsätze ordentlicher Buchführung
GoDV	Grundsätze ordentlicher Datenverarbeitung
HGB	Handelsgesetzbuch
IT	Informations-Technik; Informations-Technologie
ITIL	IT Infrastructure Library
IT/ORG	Unternehmensbereich IT und Organisation
K-Fall	Katastrophenfall
KonTraG	Gesetz für die Kostentransparenz im Unternehmen
KWG	Kreditwesengesetz
LAN	Local Area Network
MAC	Message Authentication Code
MaH	Mindestanforderungen an Handelsgeschäft (Wertpapierhandel)
NF	Notfall
OE, OEen	Organisationseinheit (Abteilung, Team)
ORG	Bereich Organisation oder Betriebsorganisation, oft gehören auch IT-Entwicklungs-Abteilungen dazu
PKI	Public Key Infrastructure
RiLi	Richtlinien
RPZ	Risikoprioritätszahl (Produkt aus Fehlerhäufigkeit, Auftretens- und Entdeckungswahrscheinlichkeit)

SLA	Service Level Agreement (vertragliche Vereinbarung)
Std.	Stunde
USV	Unterbrecherfreie Stromversorgung (Batteriepuffer für eine gewisse Zeit; in Verbindung mit einem Notstromdiesel die Überbrückungszeit, bis der Notstromdiesel Strom liefert)
WAN	Wide Area Network
WpHG	Wertpapierhandelsgesetz

Abbildungsverzeichnis

Tabellenverzeichnis

Literatur- und Quellenverweise

BSI: IT-Grundschutzhandbuch, Maßnahmenempfehlungen für den mittleren Schutzbedarf; Bundesamt für Sicherheit in der Informationstechnik; Bundesanzeigerverlag

BSI: ITIL und Informationssicherheit, Möglichkeiten und Chancen des Zusammenwirkens von IT-Sicherheit und IT-Service-Management; Studie von HiSolution AG im Auftrag des BSI

BSI: Dr. Vossbein; Kosten und Nutzen der IT-Sicherheit, Studie des BSI zur Technikfolgen-Abschätzung; SecuMedia-Verlag, 2000

Bundesministerium für Wirtschaft und Arbeit: Handbuch für den Geheimschutz in der Wirtschaft (Geheimschutzhandbuch);

BITKOM: Matrix der Haftungsrisiken, IT-Sicherheit – Pflichten und Risiken; www.bitkom.org

Claudia Eckert: IT-Sicherheit: Konzepte – Verfahren – Protokolle; Oldenbourg Verlag: 4. Aufl. 2006

Martin Wieczorek, Uwe Naujoks, Bob Bartlett (Hrsg.) Business Continuity (in Kooperation mit BCI); Springer 2002

Gero von Randow: Das Ziegenproblem, Denken in Wahrscheinlichkeiten; rororo Verlag 2004

Eigene Vorträge:

Strategie zur Optimierung der Managerhaftung bei IT-Risiken

Basel II; Was sind die kritischen Erfolgsfaktoren zur Erfüllung der Kreditanforderungen für KMUs?

Identifizieren, Bewerten und Steuern operationeller IT-Risiken

Von der unternehmensweiten Krisenstrategie zum IT-Krisenmanagement

Praktisches IT-Risk-Management; FMEA als methodischer Ansatz zur Identifizierung, Bewertung und Steuerung von operationellen Risiken

Internetdokumentation:

Bundesverwaltungsamt – Zentralstelle für Zivilschutz: Für den Notfall vorsorgen; www.bundesverwaltungsamt.de

Business Continuity Institute: Good Practice Guidelines 2008 www.thebci.org

British Standard: BS 25999-1:2006 Code of Practice www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Risk/Business-continuity/

British Standard: BS 25999-2:2007 Specification www.bsi-global.com/en/shop/Publication-Detail/?pid=0000000000030169700

BSI: BSI 100-4 Notfallmanagement
www.bsi.de/literat/bsi_standard/index.htm
BSI: Leitfaden IT-Sicherheit; IT-Grundschutz kompakt
www.bsi.de
Multimedia Initiative Hessen:
- Sicher ins Netz
- Digitale Signatur
- …

www.hessen-media.de

Links im Internet

BSI – Bundesamt für Sicherheit in der Informationstechnik
http://www.bsi.de/
BSI – SI für Bürger
http://www.bsi-fuer-buerger.de/
BUND.DE Verwaltung, Online zur Sicherheit
http://www.bund.de/sicherheit
DKKV Deutsches Komitee Katastrophenvorsorge e.V.
http://www.dkkv.org/
Fachzeitschrift für Informations-Sicherheit
http://www.kes.info/
Gesellschaft für Informatik e.V.
http://www.gi-ev.de/gliederungen/fachbereiche/sicherheit/
Krisennavigator – Institut für Krisenforschung
http://www.krisennavigator.de/
Linux Security
http://www.linuxsecurity.com/
RISKNET – THE RISK MANAGEMENT NETWORK
http://www.risknet.de/
BaFin Bundesanstalt für Finanzdienstleistungsaufsicht
http://www.bafin.de/ Suchwort „MaRisk“
Corporate Risk Management
http://www.riskbooks.de/sitemap.htm
RISIKO MANAGER
http://www.risiko-manager.com/

Index