



2009 – AUSGABE 5/6 **agens Audit & Risk Newsletter**

Informationen zu Revision,
Risikomanagement und Trainings

agens – gedacht, getan

AKTUELLES

Liebe agens Newsletter Leserinnen und Leser,

unser Team will Sie auch zum Ende dieses ereignisreichen Jahres über die Neuigkeiten im Finanzsektor informieren und Trends rund Revision, Risikomanagement und Fraud aufzeigen.

In dieser Ausgabe haben wir den Fokus auf IT Risikomanagement gesetzt. Dabei bilden die Krisenmanagementorganisation sowie BCM Notfalltest und Penetrationstests den Themenschwerpunkt.

Wir wünschen viel Spaß bei der Lektüre.



Christof Merz
(Geschäftsbereichsleiter)



Agenda

Schwerpunktthema	3
Die Krisenmanagementorganisation	3
BCM Notfalltest	7
Penetrationstests.....	11
Aktuelles.....	14
Datenschutz – Literatur für die praktische Umsetzung	14
Der „Dreiklang“ von Revision, Risikomanagement und Compliance	16
Rückblick auf die Seminare am 30.09. und 01.10.09 in Düsseldorf.....	20
Compliance Symposium 24. und 25. Februar 2010 in Hannover.....	22
Auswertung der Online-Umfrage.....	23
agens Risk Manager als Web Anwendung.....	24
Literatur	25
Seminartermine	26
Microsoft Excel.....	26
Who is Who	29
Impressum.....	30

Die Krisenmanagementorganisation

Das Business Continuity Management (BCM) ist darauf ausgerichtet, ein zielgerichtetes und effektives Handeln nach dem Eintritt eines Notfalls zu ermöglichen. Dabei handelt es sich um eine vom Normalzustand abweichende Situation, daher werden auch besondere Anforderungen an die Bewältigung dieses Vorhabens durch das Management gestellt. Für die Bewältigung dieser außergewöhnlichen Situationen wird die Einrichtung einer speziellen Krisenmanagementorganisation empfohlen. Die Krisenmanagementorganisation sollte dabei eine allgemeingültige Struktur aufweisen und für alle eintretenden „Krisensituationen“ gelten. D. h. nicht, dass die Zusammensetzung der Krisenmanagementorganisation statisch ist, es ist genau das Gegenteil. Die Zusammensetzung sollte immer die speziellen Anforderungen der eingetretenen Situation oder Krise berücksichtigen. Die Erweiterung oder Reduzierung dieser Organisation sollte anforderungsgerecht erfolgen, so dass möglichst immer die für die Behandlung der speziellen Sachverhalte erforderliche Expertise in dem Gremium vertreten ist, um die anstehenden Aufgaben zielgerichtet und effizient bearbeiten zu können. Durch diese Flexibilität in der Besetzung wird auch die Größe des Gremiums an den aktuellen Bedarf angepasst, dabei geht es um kurze Entscheidungswege und eine anforderungsgerechte Handlungsweise zur Bewältigung von Krisen. Die bestehende Linienorganisation ist dafür wenig geeignet, da diese i. d. R. zu bürokratisch bzw. zu träge ist, um zügig und zielgerichtet Entscheidungen zu treffen und deren Umsetzung zu veranlassen.

Der Begriff „Krise“ definiert eine unvorhersehbare Situation, für die keine Maßnahmenplanung bis ins Detail vorab erstellt werden kann. Eine einmal bewährte Lösung führt in einer weiteren Krisensituation nicht zwangsläufig zum gewünschten Erfolg. Ein Fehler in einer Steuerungssoftware kann bspw. beim ersten Mal harmlos sein, beim zweiten Mal jedoch eine existenzielle Bedrohung darstellen, wenn eine vollständige Rückrufaktion für alle ausgelieferten Produkte erforderlich wird.

Krisen entwickeln häufig eine Eigendynamik, die in verschiedene Richtungen gehen kann, die zwar vorstellbar, aber nicht detailliert vorausplanbar sind. Einzig planbar ist die Krisenmanagementorganisation mit organisatorischen und operativen Hilfsmitteln sowie die dazugehörige Alarmierung und Eskalation. Eine Krise kann vielfältige Ursachen haben und ist bspw. dadurch gekennzeichnet, dass unter Zeitdruck, Anspannung, Angst und bei bestehenden Unsicherheiten die dringend notwendigen Handlungsentscheidungen für die Zukunft zu treffen sind. Das Ziel besteht darin, die Krise schnellstmöglich in den Griff zu bekommen und einen negativen Verlauf abzuwenden. Entscheidend für eine erfolgreiche Krisenbewältigung sind vor allem die ersten eingeleiteten Maßnahmen.

Demgegenüber stellt ein „Notfall“ den Eintritt eines definierten Szenarios mit einer Störung größeren Ausmaßes dar, typischerweise einen Ausfall des gesamten Rechenzentrums oder eines zentralen Gebäudes. Als Folge davon kann ein Großteil der Geschäftsprozesse des Unternehmens nicht mehr ordnungsgemäß weitergeführt werden. Sind keine vorsorglichen Maßnahmen für den Wiederanlauf der Geschäftsprozesse getroffen worden, ist mit spürbaren negativen Auswirkungen für die Stakeholder, Kunden, Geschäftspartner und das eigene Unternehmen zu rechnen. Das kann im Extremfall auch dazu führen, dass der Fortbestand des Unternehmens gefährdet ist. Die Bewältigung von Notfällen ist Aufgabe der Krisenmanagementorganisation.

Krisenmanagement bedeutet, unternehmenskritische Entwicklungen durch ein Höchstmaß an Prävention möglichst im Vorfeld zu verhindern und durch den Einsatz aller verfügbaren personellen, organisatorischen und technischen Mittel „das Schlimme zum Guten zu wenden“. Sei es durch die einfache geniale Idee des erfahrenen Krisenmanagers, durch die Bewertung und Auswahl von zielgerichteten Handlungsalternativen oder durch Rückgriff auf vorbereitete Maßnahmen wie im BCM.

SCHWERPUNKTHEMA

Ein professionelles Krisenmanagement setzt eine Auseinandersetzung mit den unternehmensspezifischen Risiken voraus. Dafür ist ein ganzheitliches Risikomanagement erforderlich. Das Krisenmanagement besteht aus dem vollständigen Erfassen der Krise und der Entwicklung von zeitgerechten und adäquaten Reaktionen. Jede Krise hat ihre individuelle Ausprägung und es gibt nicht den Masterplan zur Bewältigung von Krisen. Es gibt jedoch bewährte Erkenntnisse und Regeln, die beachtet werden sollten bevor die Krise eintritt. Hierzu gehört die Etablierung eines Krisen- oder Notfallstabes, der für die Lösung der gestellten Aufgabe personell, organisatorisch und logistisch ausreichend ausgestattet und vorbereitet sein sollte. Dazu gehört bspw., dass der Krisenstab seine Tätigkeit in der Krisenstabszentrale aufnimmt.

Die Größe der Krisenmanagementorganisation hängt von der Größe und Struktur des Unternehmens ab und sollte darauf angepasst sein. In einer Konzernstruktur kann es bspw. einen Krisenstab auf der Konzernebene und jeweils einen Krisenstab in jeder Konzerngesellschaft geben. Die Zuständigkeiten der Krisenstäbe beziehen sich dabei auf die jeweilige Gesellschaft, wobei der Konzernkrisenstab die höchste Instanz bildet und Weisungsbefugnis gegenüber den Krisenstäben in den Konzerngesellschaften besitzt. Umgekehrt besteht eine Informations- und Berichtspflicht an den Konzernkrisenstab. Bei kleineren Organisationen wird es nur einen Krisenstab geben und die Funktionen werden auch nicht mit Teams aus mehreren Personen besetzt sein, sondern es wird vermutlich Personen geben, die mehrere Funktionen ausüben.

Der Aufbau der Krisenmanagementorganisation ist durch die Definition von Funktionen/Rollen gekennzeichnet, wie es grundsätzlich für das BCM zu empfehlen ist. Das bietet den Vorteil, einer weitgehend statischen Struktur, selbst wenn die Personen wechseln, die die Funktionen besetzen. Die nachfolgende Abbildung zeigt ein Beispiel für eine Krisenmanagementorganisation.

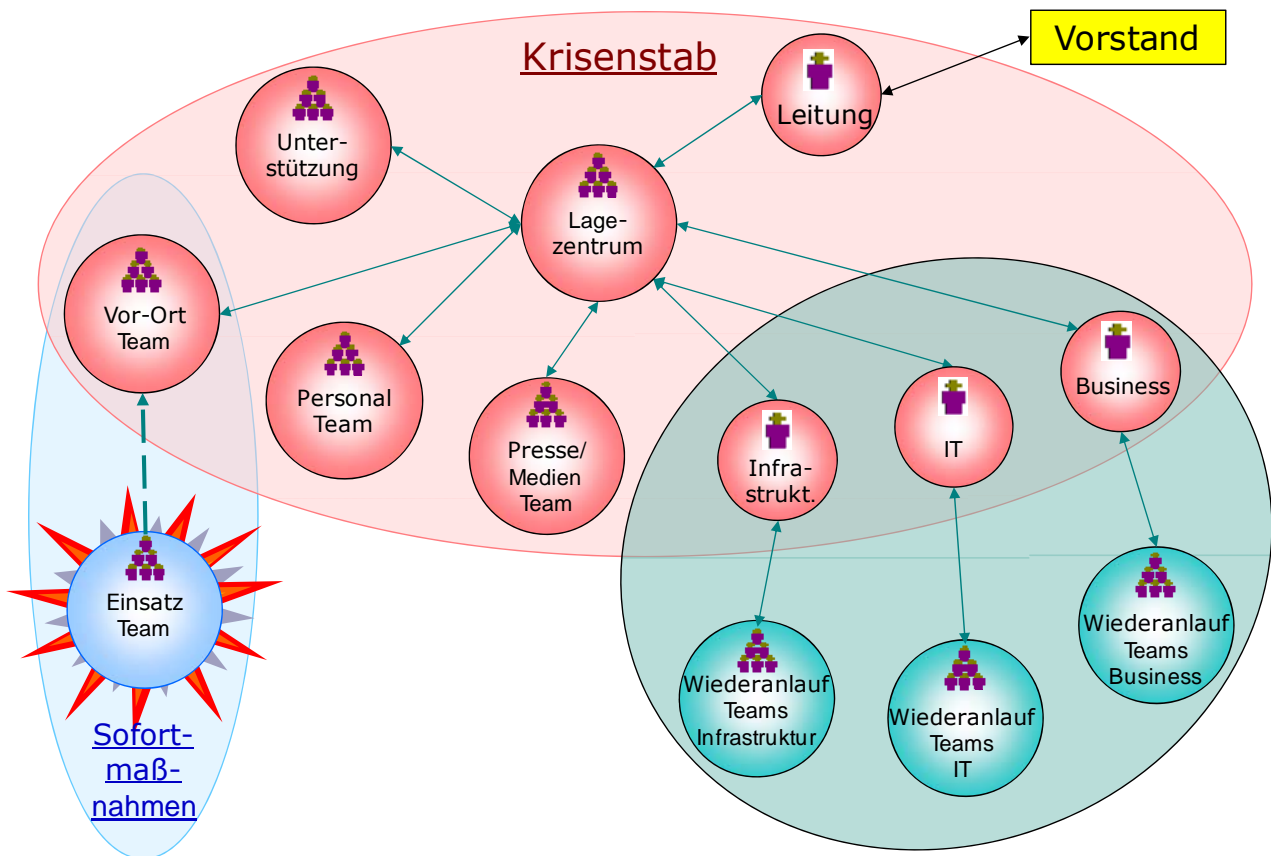


Abb. 1: Beispiel einer Krisenmanagementorganisation

SCHWERPUNKTHEMA

Bei der Besetzung der Funktionen oder Teams, in Abhängigkeit von der Größe des Unternehmens, ist darauf zu achten, dass die Personen über die erforderlichen Qualifikationen verfügen. Bspw. psychische und physische Belastbarkeit, analytische Fähigkeiten, Entscheidungsfreudigkeit, Team- und Kommunikationsfähigkeit. Dabei muss nicht zwangsläufig jede Funktion mit einer Person besetzt sein, es ist auch vertretbar, wenn einige Personen mehrere Funktionen innehaben, sofern dadurch keine Überlastung erfolgt.

Die Besetzung sollte grundsätzlich funktionsorientiert und nach der Kompetenz erfolgen, nicht notwendigerweise hierarchisch. Es ist zu beachten, dass die unternehmensindividuellen Anforderungen erfüllt werden und die Einsatzfähigkeit erhalten bleibt. Die Örtlichkeiten, an denen die Funktionsträger präsent sein müssen, sind dabei ebenfalls zu berücksichtigen. Die Übertragung des Mandats für das Krisenmanagement an die bestehende Managementstruktur ist meist keine geeignete Option. Der Stab der Krisenmanagementorganisation sollte so klein wie möglich und so ausbaufähig wie nötig sein. Jede wichtige Funktion ist zwingend mit einem Stellvertreter zu besetzen. Für mittlere und große Unternehmen empfiehlt es sich, die Organisationsstruktur in drei Ebenen zu gliedern:

- Ebene 1 (strategisch) – Entscheidungsebene, die üblicherweise von dem Vorstandsvorsitzenden, den Vorstandsmitgliedern oder den Geschäftsführern gebildet wird,
- Ebene 2 (taktisch) – Krisenstab, der die strategischen Entscheidungen koordiniert und umsetzt,
- Ebene 3 (operativ) – lokale Notfallteams für die Umsetzung der Maßnahmen und Ausführung von fachlichen Tätigkeiten.

Die Grundlagen für die Krisenmanagementorganisation sind in einer Policy zu definieren, die den Rahmen für die Ausgestaltung bildet. Das Krisenmanagementhandbuch enthält die Verfahrensbeschreibung, darin enthalten sind bspw. mögliche Szenarien für Krisen, Verantwortlichkeiten, Weisungsbefugnisse, zu besetzende Funktionen mit/ohne Stimmrecht, Aufgaben der einzelnen Funktionen, Kriterien für die Alarmierung und Einberufung, Voraussetzung für die Beschlussfähigkeit, Regelung der zusätzlich erforderlichen Kompetenzen um agieren zu können, Regeln für die Hinzuziehung von Experten, verfügbare Krisenstabszentralen, Lagepläne, das Change Management Verfahren etc.

Die Ausstattung der Krisenstabzentralen sollte sorgfältig geplant werden, um bspw. über die benötigten Räume mit Büroausstattung und die erforderliche technische Ausstattung zu verfügen. Der Krisenstab sollte schließlich möglichst ungestört, diskret und effizient arbeiten können.

Wird die Krisenmanagementorganisation durch das Alarmierungs- und Eskalationsverfahren aktiviert, so übernimmt der Krisenstab die Zuständigkeit und Entscheidungskompetenz. Der Krisenstab bestimmt die Bereiche, die durch die Krise betroffen sind und befasst sich nur mit diesen Bereichen. Das hat zur Folge, dass in den betroffenen Bereichen die Linienorganisation außer Kraft gesetzt wird und die Managementverantwortung an den Krisenstab übergeht. Außerhalb der betroffenen Bereiche bleibt weiterhin die Linienorganisation erhalten und tätig.

In der ersten Sitzung des Krisenmanagements geht es um die Erstellung einer Lagebeurteilung und die Einleitung der ersten Maßnahmen. D. h. bspw. für das BCM, dass die Entscheidung zu treffen ist, ob ein Notfall entsprechend der definierten Szenarien vorliegt und die dafür vorbereiteten Wiederanlaufmaßnahmen 1:1 oder in abgewandelter Form durchzuführen sind.

Nach der Einleitung und Umsetzung dieser Maßnahmen geht es um die Beobachtung der weiteren Entwicklungen und die Durchführung von turnusmäßigen Lagebestimmungen, um ggf. korrigierende Maßnahmen einzuleiten, die für die Etablierung und Durchführung eines stabilen Notbetriebs unerlässlich sind. Parallel dazu bzw. zeitlich nachgelagert erfolgt die Schadensaufnahme und -bewertung. Daraus leiten sich die erforderlichen Maßnahmen ab, die erforderlich sind, um aus dem Notbetrieb wieder in den Normalbetrieb zu gelangen. Hat sich die Lage ent-

SCHWERPUNKTHEMA

sprechend stabilisiert kommt der Zeitpunkt, wo über die Deaktivierung der Krisenmanagementorganisation entschieden wird.

Im Krisenstab sind alle wesentlichen Ereignisse und Beschlüsse chronologisch zu protokollieren, um nachweisen zu können, auf welcher Grundlage die Entscheidungen getroffen wurden. Die Ordnungsmäßigkeit und Nachvollziehbarkeit der Handlungen steht dabei im Vordergrund.

Als Vorbereitung auf diese außergewöhnliche Situation ist es unbedingt erforderlich, ein Krisenmanagementhandbuch mit den relevanten und praktikablen Informationen für das Unternehmen zu erstellen. Darin sollten bspw. auch entsprechende Checklisten für die einzelnen Funktionen enthalten sein, die zur Orientierung und Durchführung der wesentlichen Aufgaben verwendet werden können. Dazu gehören bspw. Checklisten zur Lagebeurteilung, vorbereitete Presseerklärungen, Mitteilungen an die Eigentümervertretung, Aufsichtsrat, Aufsichtsbehörden, Geschäftspartner, Kunden, Übersichten mit Kontaktadressen etc.

Damit der Krisenstab nicht unvorbereitet in die Bewältigung von Krisen gerät sind Sensibilisierungs- und Schulungsmaßnahmen durchzuführen. Alle Mitglieder der Krisenmanagementorganisation sind zudem verpflichtet, sich mit dem Inhalt des Krisenmanagementhandbuchs vertraut zu machen. Außerdem ist die Durchführung von Krisenmanagementübungen zu empfehlen, um mögliche Krisensituationen zu trainieren und Krisenkompetenz aufzubauen.

Ansprechpartner: Norbert Neben (Senior Berater)

SCHWERPUNKTHEMA

BCM Notfalltest

Jedes Vorhaben muss sich in der Praxis bewähren, um einen Mehrwert zu erzeugen, nutzbringend einsetzbar zu sein, Akzeptanz zu erreichen oder auch um den Nachweis zu führen, dass die getätigten Investitionen einen Nutzen erbringen. Das gilt ebenso für das Business Continuity Management (BCM). Das Vorhaben wurde initiiert, um sich auf den möglichen Eintritt von Notfällen vorzubereiten. Es gilt die unternehmenskritischen Geschäftsprozesse abzusichern, um den Fortbestand des Unternehmens, durch die Aufrechterhaltung der Wertschöpfungskette, zu gewährleisten. Dabei wird bewusst davon ausgegangen, dass Schäden eintreten können, aber diese dürfen keine unternehmenskritischen Dimensionen erreichen, um das Unternehmen nicht in eine kritische Phase zu führen, die mit unkalkulierbaren Risiken verbunden ist.

Das BCM ist kein Projekt, sondern ein Prozess der kontinuierlich fortentwickelt und den Veränderungen im Unternehmen folgen muss. Dabei ist es egal, ob neue Geschäftsfelder aufgebaut oder Produkte ausgemustert werden, ob sich der Umsatz im Produktportfolio gravierend verschiebt oder gesetzliche bzw. eigene Richtlinien verändert werden. Das alles muss sich im BCM widerspiegeln, um auf die geschäftskritischen Prozesse fokussiert zu bleiben und gilt in gleicher Weise für die Notfalltests.

Ist das BCM im Unternehmen etabliert gilt es den Nachweis zu erbringen, dass es praxistauglich ist und den gewünschten Nutzeffekt erbringt. Das Papier ist geduldig und darauf zu hoffen, dass ein nicht getestetes Verfahren im Notfall schon planmäßig funktionieren wird, ist fahrlässig, das zeigt sich immer wieder bei der Durchführung von Notfalltests. Nur was in der Praxis erfolgreich getestet wurde hat den Nachweis der Funktionsfähigkeit erbracht.

Die gesetzlichen Auflagen zur Notfallvorsorge sind schon seit längerer Zeit existent, bspw. KonTrag, MaRisk BA und seit kurzem auch MaRisk VA. Somit sind alle Unternehmen aufgefordert nicht nur das BCM im Unternehmen umzusetzen, sondern auch regelmäßig die Wirksamkeit und Angemessenheit des Notfallkonzeptes durch Notfalltests zu überprüfen. Die Ergebnisse der Notfalltests sind zu dokumentieren und den jeweiligen Verantwortlichen mitzuteilen.

Aufgrund der Anforderungen, die sich aus den MaRisk ableiten, ist erkennbar, das BCM immer enger mit den Bereichen Compliance und Risikomanagement in Verbindung gebracht wird. Dieser Aspekt sollte auch bei der organisatorischen Eingliederung des BCM in die Organisationsstruktur entsprechende Berücksichtigung finden.

Für die Durchführung von Notfalltests sind entsprechende Ressourcen sowie ein Budget einzuplanen, daher sollte eine kurz- und mittelfristige Planung erfolgen. Die kurzfristige Planung, z. B. für das Kalender- oder Geschäftsjahr sollte konkret sein und die geplanten Notfalltest mit Terminen und Ressourcen beinhalten. Die mittelfristige Planung, z. B. für die beiden darauf folgenden Jahre, sollte einer Grobplanung entsprechen. Ohne eine vorausschauende Planung ist häufig schon die Terminierung von Notfalltests schwierig, das gilt besonders für die Notfalltests, an denen die IT maßgeblich beteiligt ist.

Die IT-Servicezeiten liegen heute in vielen Fällen bei 7 x 24h, außerdem sind Wartungsarbeiten einzuplanen und durchzuführen. Es werden bspw. IT-Systeme erweitert oder ausgetauscht, es sind Veränderungen an der Infrastruktur (Strom, Klima, USV, Netzersatzanlage) erforderlich und die Fachabteilungen benötigen Wartungsfenster, um neue Anwendungen einzuführen (Test- und Freigabeverfahren). In den meisten Fällen ist es daher schwierig freie Termine zu finden, häufig müssen Terminverschiebungen erfolgen, um Notfalltests einplanen zu können - besonders dann, wenn ein normales Wochenende für die Durchführung des Notfalltests nicht ausreicht und zusätzliche Testzeit vor oder nach dem Wochenende erforderlich ist.

Inhaltlich sollten im BCM-Testplan alle Notfalltests berücksichtigt werden, die dem BCM zugeordnet werden können. Hierzu zählen z. B. auch Alarmierungs- und Räumungsübungen, um

SCHWERPUNKTHEMA

eine vollständige Sicht über alle geplanten Notfalltests zu bekommen. Wichtig ist bei der Planung der Notfalltests, sich nicht nur auf die IT zu fokussieren, denn das BCM wird maßgeblich durch die Geschäftsprozesse geprägt. Das erfordert die Ausführung entsprechender Tätigkeiten durch die Fachbereiche. Daraus resultiert, dass Notfalltest ohne die Einbeziehung der Fachbereiche unvollständig bleiben und somit kein vollständiger Nachweis über die Verlässlichkeit der Notfallvorsorge, d. h. die Absicherung der unternehmenskritischen Geschäftsprozesse, zu erbringen ist.

Das soll jedoch nicht heißen, dass beim ersten Notfalltest alles vollumfänglich und mit der Beteiligung aller betroffenen Fachbereiche getestet werden sollte. Es ist zu empfehlen, den Umfang für die ersten Notfalltests zunächst auf Teilbereiche zu beschränken und iterativ zu planen. Nach der erstmaligen Erstellung der Notfallpläne ist davon auszugehen, dass eine Reihe von Unsicherheiten und Risiken bestehen. Die in der Theorie erarbeiteten Notfallpläne beinhalten vermutlich auch noch Fehler und somit ist eine erfolgreiche Durchführung beim ersten Notfalltest nicht gewährleistet. Zudem ist es für alle Beteiligten mit einer größeren Motivation verbunden, wenn Erfolge erzielt werden, selbst dann, wenn die Auswertung des Notfalltests zeigt, dass noch nicht alles optimal verlaufen ist und nur Teilziele erreicht wurden.

Die Planung der Notfalltests sollte auch immer unter Risikogesichtspunkten erfolgen, d. h. den Schwerpunkt bilden die Bereiche mit hohem Risikopotenzial. Daher bietet es sich an, das Risikomanagement oder auch andere relevante Bereiche des Unternehmens bei der Planung von Notfalltests mit einzubeziehen. Innerhalb einer Planungsperiode sollten die unternehmenskritischen Geschäftsprozesse vollständig abgedeckt werden.

Die Unternehmensbereiche, für die besondere gesetzliche oder auch interne Vorgaben gelten, müssen dabei entsprechend berücksichtigt werden. Das sind bspw. der Zahlungsverkehr (Kreditwesengesetz – KWG) und der Wertpapierhandel (Wertpapierhandelsgesetz – WpHG) bei den Kreditinstituten. Zudem sollten bei wiederkehrenden Notfalltests die Anforderungen kontinuierlich gesteigert und/oder andere Bereiche miteinander kombiniert werden. Bspw. kann ein Notfalltest mit der Alarmierung und Einberufung des Krisenstabs kombiniert werden. Es sollte das Ziel sein, die definierten Notfallszenarien in einem Notfalltest möglichst vollständig abzudecken. Ist der dafür erforderliche Aufwand nicht tragbar, so werden Teilbereiche nacheinander oder in unterschiedlichen Kombinationen getestet. Dabei sollten zusammengehörige Bereiche auch gemeinsam getestet werden.

Es geht dabei schließlich um das Sammeln von Erfahrung und die kontinuierliche Vertiefung der Kenntnisse, die zu einer erfolgreichen Ausführung der Notfallpläne erforderlich sind. Außerdem sind praktische Erfahrungen hilfreich, um Unsicherheiten im Umgang mit Notfallplänen oder auch Ängste abzubauen. Es ist das Ziel auf den Eintritt eines Notfall optimal vorbereitet zu sein, d. h. bspw. das im Notfallteam der Fachabteilung A, ein klares Verständnis darüber besteht, welche Tätigkeiten für den Geschäftsprozess X wichtig und mit welcher Priorität abzuarbeiten sind und auf welche Tätigkeiten im Notbetrieb zunächst verzichtet werden kann. Dabei ist die Einhaltung von ggf. vorgegebenen Fristen und Terminen zu berücksichtigen.

Der Aufwand für die Planung und Vorbereitung von Notfalltests variiert stark in Abhängigkeit von Umfang und Komplexität des geplanten Notfalltests und der vorhandenen IT-Umgebung. Soll bspw. in einer IT-Hochverfügbarkeitslösung, die auf zwei Rechenzentrumsstandorte verteilt ist, der Ausfall eines Standortes simuliert werden, um zu überprüfen, ob die unternehmenskritischen Anwendungen in der geforderten Wiederanlaufzeit aus dem verbleibendem RZ-Standort zur Verfügung gestellt werden können, so ist mit einem hohen Vorbereitungsaufwand zu rechnen. Für solche komplexen IT-Umgebungen kann die Planung eines Notfalltests durchaus mehrere Monate beanspruchen.

Besonders aufwändig gestalten sich häufig die vollständige Trennung der beiden RZ-Standorte und der Schwenk der Kommunikationsverbindungen (Daten und Sprache) auf das RZ in dem der Notfalltest durchgeführt wird. Die Verbindungen zu Filialen, Geschäftspartnern, Dienstleis-

SCHWERPUNKTHEMA

tern, Internet etc. sollen schließlich auch im Test zur Verfügung stehen. Tritt ein realer Notfall mit dem vollständigen Ausfall eines RZ-Standortortes ein, entfallen diese Tätigkeiten, da keine Standorttrennung erforderlich ist. Für den Notfalltest müssen diese Tätigkeiten jedoch eingeplant werden. Daraus resultieren entsprechende Aufwände in der Vorbereitung. Die IT-Umgebung muss für den Notfalltest vorbereitet werden, der Notfalltest ist durchzuführen und danach ist die vollständige Wiederherstellung der Produktionsumgebung für den nächsten Werktag erforderlich. Es ist schließlich das Ziel, den Notfalltest ohne negative Auswirkungen auf die Produktion durchzuführen. Diese Erwartung liegt im Interesse des Unternehmens und ist aus Sicht der Kunden berechtigt. Daher sind eine sorgsame Vorbereitung, Durchführung und Nachbereitung unabdingbar.

Auch auf Seiten der Fachbereiche kann sich die Planung und Vorbereitung von Notfalltest entsprechend umfangreich gestalten. Sollen bspw. die wesentlichen Geschäftsprozesse von den Fachabteilungen im Notfall- oder Ausweichrechenzentrum überprüft werden, so resultierten daraus entsprechende Aufwände. Die verfügbaren Zeitfenster für die Durchführung der Notfalltests sind häufig knapp bemessen, bspw. muss die Wochenverarbeitung und Datensicherung abgeschlossen sein, bevor der Notfalltest gestartet werden kann. Es ist daher kaum mehr möglich mit Testdaten zu arbeiten.

Die Durchführung des Notfalltests mit Produktivdaten stellt wesentlich höhere Anforderungen, da der gesamte Produktionsprozess fehlerfrei durchlaufen werden muss. Im Vorwege ist es daher erforderlich, dass die Fachabteilungen repräsentative Geschäftsvorfälle selektieren, bei denen möglichst alle Prozessschritte enthalten sind, um eine vollumfängliche Bearbeitung der Geschäftsvorfälle nachweisen zu können. Das bedeutet in vielen Fällen, dass nach der eigentlichen Verarbeitung ein Output in Form von Mitteilungen, Briefen, Auszügen etc. erstellt, gedruckt und dem Postversand zugeführt werden muss. Dieses wiederum erfordert z. B., dass die Online-Verarbeitung abgeschlossen sein muss, um die Batchverarbeitung starten zu können. Ist die Batchverarbeitung abgeschlossen sind häufig Kontrollen und Freigaben durch die Fachabteilungen erforderlich, bevor die Nachverarbeitung im Druckzentrum und die Kuvertierungen erfolgen können.

Bei umfangreichen Vorhaben ist daher die Planung und Durchführung eines Notfalltests als Projekt unabdingbar. Dabei ist ein analoges Vorgehen wie bei Projekten zu empfehlen, d. h. auch ein Notfalltest sollte entsprechend beantragt, geplant und freigegeben werden. Im Antrag selbst sind Auftraggeber, Auftrag, Ziel, Meilensteine, Termine, Voraussetzungen, Risiken, benötigte Ressourcen etc. zu dokumentieren. Diese Vorgehensweise ist generell zu empfehlen, auch weniger komplexe Notfalltests sollten in strukturierter Form geplant werden. Für die einzelnen Projektphasen eines Notfalltests – Beantragung, Freigabe, Planung, Durchführung, Auswertung und Überwachung der Folgemaßnahmen, bietet sich die Entwicklung von entsprechenden Vorlagen bzw. Templates an.

Die Einzeldokumente können sehr vorteilhaft in ein Testhandbuch integriert werden, in dem das generelle Vorgehen zur Durchführung von Notfalltests dokumentiert ist. Hierzu gehören auch entsprechend vorbereitete Checklisten für die Testdurchführung, um die Ergebnisse und Abweichungen zu protokollieren. Als Werkzeuge für das Projekt Notfalltest können die gängigen MS Office Produkte eingesetzt werden. Ist eine BCM-Software im Einsatz, so empfiehlt es sich zu prüfen, ob das Softwareprodukt hilfreiche Unterstützung bei der Planung, Durchführung und Auswertung bietet. Ist der Notfalltest sehr komplex und umfangreich und bestehen viele Anhängigkeiten zwischen den einzelnen Aktivitäten, so ist eine Durchführung ohne Einsatz einer BCM-Software häufig sehr aufwändig und schwierig.

Sind die geplanten Notfalltests mit hohen Kosten und/oder hohen Risiken behaftet, so kann es durchaus sinnvoll sein, von Beginn an die Interne Revision oder auch externe Berater in das Projekt mit einzubeziehen. Die Durchführung einer projektbegleitenden Prüfung reduziert die Risiken und führt zu einer neutralen Sichtweise und Bewertung der einzelnen Phasen des Notfalltests. Hieraus ergeben sich häufig wertvolle Hinweise für Optimierungsmaßnahmen und

SCHWERPUNKTHEMA

zur Effizienzsteigerung. Das ist auch zu empfehlen, wenn die erreichten Ergebnisse aus vorherigen Notfalltests weit von der Zielvorstellung abweichen oder nach der Durchführung von wesentlichen Veränderungen in der IT-Umgebung oder Organisation.

Bei der Durchführung von Notfalltests sind neutrale Beobachter oder Protokollanten mit einzuplanen, die das Vorgehen, wesentliche Ereignisse, Planabweichungen, erzielte Ergebnisse dokumentieren und eine Bewertung zum Notfalltest erstellen, die mit den beteiligten Fachabteilungen abgestimmt wird. Die Mitarbeiter, die direkt in die Durchführung des Notfalltests einbezogen sind, können das nur sehr eingeschränkt leisten, da diese mit den fachlichen Aufgaben, Bearbeitung von Problemen, Abstimmungen zwischen den einzelnen Teams etc. bereits ausgelastet sind.

Die Auswertung von Notfalltests sollte in sachlicher Weise die festgestellten Schwachstellen aufzeigen, entsprechende Maßnahmen zu deren Beseitigung enthalten und auch Hinweise für weitere Notfalltests beinhalten. Der daraus abgeleitete Maßnahmenkatalog ist zudem mit Terminen und Verantwortlichkeiten zu versehen, um eine Maßnahmenverfolgung zu ermöglichen.

Jeder Notfalltest bietet zudem die Möglichkeit, einen Erfahrungsbericht zu erstellen und zu publizieren, um das Bewusstsein zum Thema BCM im gesamten Unternehmen zu fördern und die Bedeutung zu unterstreichen. Das kann durch eine aktive Teilnahme von Krisenstabsmitgliedern bzw. Unternehmensmanagement an den Notfalltests noch verstärkt werden. Nur erfolgreich durchgeführte Notfalltests liefern die Nachweise, dass die Notfallpläne zum Ziel führen.

Ansprechpartner: Norbert Neben (Senior Berater)

Penetrationstests

Bei der Nutzung öffentlicher Netzstrukturen sehen sich Unternehmen vielfältigen Gefährdungen gegenüber. Es sind die komplexen Informations- und Kommunikationsstrukturen, die sich den Unternehmen nicht ganzheitlich erschließen und auf die teilweise nur unwesentlich oder überhaupt nicht Einfluss genommen werden kann. Unternehmen schließen sich an das Internet an und geben damit einen Teil ihrer direkten Verantwortung ab, ebenso setzen sie sich damit neuen Bedrohungen insbesondere für die IT-Systeme aus, auf die angemessen reagiert werden muss.

Für potenzielle Täter können unterschiedliche Motivationen ausschlaggebend sein, Angriffe auf IT-Systeme durchzuführen. Während „Hacker“ als experimentierfreudige Programmierer angesehen werden, die sich aus technischem Interesse mit Sicherheitslücken in IT-Systemen auseinandersetzen, werden unter „Crackern“ Personen verstanden, die sich aufgrund krimineller Energie der Schwachstellen von IT-Systemen bedienen, um dadurch rechtswidrige Vorteile oder gesellschaftliche Aufmerksamkeit bzw. Anerkennung zu erlangen.

Es existieren mehrere Möglichkeiten, IT-Systeme in ihrer Funktionsweise zu manipulieren oder zu schädigen bzw. einen Angriff auf IT-Systeme vorzubereiten. Bei Angriffen über das Netzwerk erfolgen Attacken unter der Nutzung von Funktionalitäten der eingesetzten Netzwerkprotokolle auf Netzwerkkomponenten, Computersysteme bzw. Applikationen. Diese Art von Angriffen macht sich Schwachstellen in Hard- und Software zunutze. Bei sog. Social-Engineering-Angriffen wird versucht, Mitarbeiter des Unternehmens mit privilegiertem Wissen insofern zu manipulieren, dass sie dem Angreifer sicherheitsrelevante Informationen, wie z. B. Passwörter, preisgeben. Wenn physische Sicherheitsmaßnahmen überwunden werden können und auf diese Weise physischer Zugriff auf die IT-Systeme erlangt wird, ist es meist nur eine Frage der Zeit, bis auch ein Zugriff auf bzw. die Manipulation der gespeicherten Anwendungen und Daten stattfinden kann.

Um den beschriebenen Gefahren entgegenzuwirken, ergreifen Unternehmen technische und organisatorische Maßnahmen zur Steigerung der IT-Sicherheit. Eine hoch wirkungsvolle technische Maßnahme ist der Penetrationstest. Durch ihn kann geprüft werden, ob die IT-Sicherheit durch die aktuell eingesetzten Sicherheitsmaßnahmen gewährleistet ist und inwieweit sie durch Bedrohungen von Hackern gefährdet ist.

Die Ziele eines Penetrationstests sind die Identifikation von Schwachstellen, das Aufdecken potenzieller Fehler, die sich aus der Bedienung bzw. Parametrisierung der IT-Systeme ergeben, die Erhöhung der Sicherheit auf technischer und organisatorischer Ebene sowie die Bestätigung der IT-Sicherheit durch einen externen Dritten.

Der Penetrationstest ist ein simulierter, realitätsnaher Hackerangriff. Während ein Vulnerability bzw. Security Scan weitgehend automatisch abläuft, wird beim Penetrationstest ein wesentlich größerer Teil der möglichen Angriffsattacken manuell erbracht und die Tester versetzen sich in die Rolle eines Hackers.

Entsprechend bedarf es bei einem Penetrationstest manueller Vorbereitung in Form von Sichtung des Prüflings, Planung der Testverfahren und -ziele, Auswahl der notwendigen Werkzeuge und schließlich der Durchführung.

SCHWERPUNKTHEMA

Die Methodik für die Durchführung von Penetrationstests gliedert sich in folgende fünf Phasen:

- Phase 1: Vorbereitung
- Phase 2: Informationsbeschaffung und -auswertung
- Phase 3: Bewertung der Informationen/Risikoanalyse
- Phase 4: Aktive Eindringversuche
- Phase 5: Abschlussanalyse

Phase 1: Vorbereitung

Zu Beginn eines Penetrationstests müssen die Ziele definiert werden. Ziele eines Penetrationstests sind die Identifikation von Schwachstellen, das Aufdecken potenzieller Fehler, die sich aus der (fehlerhaften) Bedienung ergeben, die Erhöhung der Sicherheit auf technischer und organisatorischer Ebene und die Bestätigung der IT-Sicherheit durch einen externen Dritten. Im Zuge dessen sind auch die Risiken zu berücksichtigen, die die Durchführung eines Penetrationstests mit sich bringt. Werden die relevanten gesetzlichen Bestimmungen nicht vollständig berücksichtigt, könnte dies straf- und/oder zivilrechtliche Konsequenzen nach sich ziehen. Deshalb muss sichergestellt sein, dass mit den Prüfungshandlungen nicht gegen gesetzliche Bestimmungen bzw. vertragliche Vereinbarungen verstoßen wird. Werden Penetrationstechniken nicht mit der IT abgestimmt oder Risiken der eingesetzten Techniken nicht ausreichend kommuniziert, droht möglicherweise der Ausfall von Produktsystemen. Das Vorgehen und die daraus resultierenden Risiken sind im Vorfeld zu besprechen und zu dokumentieren.

Phase 2: Informationsbeschaffung und –Auswertung

Nachdem Ziele, Umfang, Vorgehen, Notfallmaßnahmen etc. unter Berücksichtigung der rechtlichen bzw. organisatorischen Aspekte sowie der sonstigen Voraussetzungen definiert worden sind, kann mit der Sammlung von Informationen über das Ziel begonnen werden. Diese Phase wird auch als passiver Penetrationstest bezeichnet. Ziel ist es, eine möglichst komplette und detaillierte Übersicht über die installierten Systeme inklusive der potenziellen Angriffspunkte bzw. der bekannten Sicherheitsmängel zu erlangen. Je nach Anzahl der zu untersuchenden Systeme bzw. nach Größe des zu untersuchenden Netzwerkes können die Prüfungsschritte mitunter sehr zeitaufwändig werden.

Phase 3: Bewertung der Informationen/Risikoanalyse

Ein erfolgreiches, nachvollziehbares und vor allem ein wirtschaftlich effizientes Vorgehen muss die gesammelten Informationen analysieren und bewerten, bevor die zum Teil sehr zeitaufwändigen Prüfungsschritte zum aktiven Eindringen durchgeführt werden. In die Bewertung müssen die vereinbarten Ziele des Penetrationstests, die potenzielle Gefährdung der Systeme und der geschätzte Aufwand für das Evaluieren der potenziellen Sicherheitsmängel für die nachfolgenden aktiven Eindringversuche einfließen. Anhand dieser Bewertung werden dann die Angriffsziele für Phase 4 ausgewählt. So können z. B. aus der Liste der identifizierten Systeme für das weitere Vorgehen nur solche ausgewählt werden, für die aufgrund ihrer Konfiguration bzw. der identifizierten Applikationen/Dienste potenzielle Schwachstellen bekannt sind oder solche, bei denen ein Tester beispielsweise über besonders detaillierte Kenntnisse verfügt. Bei einem Penetrationstest, bei dem schon für Phase 2 eine genau definierte Anzahl von Zielsystemen vereinbart wurde, bedeutet die Auswahl faktisch eine Reduktion der Zielsysteme für Phase 4.

SCHWERPUNKTHEMA

Phase 4: Aktive Eindringversuche

Schließlich werden die ausgewählten Systeme aktiv angegriffen. Diese Phase birgt das größte Risiko innerhalb eines Penetrationstests und sollte daher mit der nötigen Sorgfalt durchgeführt werden. Hier zeigt sich aber erst, inwieweit die vermeintlichen Schwachstellen, die im Rahmen der Informationsbeschaffung identifiziert wurden, tatsächliche Risiken darstellen. Falls eine Verifikation der potenziellen Schwachstellen gefordert ist, muss diese Prüfungsphase durchgeführt werden. Bei Systemen, an die sehr hohe Ansprüche an die Verfügbarkeit bzw. an die Integrität gestellt werden, müssen vor Durchführung von kritischen Prüfungshandlungen, die möglichen Konsequenzen jeweils genau abgewogen werden. Im Rahmen eines White-Box Test muss bei kritischen Systemen vor der Durchführung des Tests ein eventuell verfügbarer Patch installiert werden, um einen Ausfall zu verhindern. Die Prüfung wird dann wahrscheinlich keine Schwachstelle feststellen können, dafür aber die Sicherheit des Systems dokumentieren.

Phase 5: Abschlussanalyse

Neben den Aufzeichnungen der einzelnen Prüfungsschritte sollte der Abschlussbericht auch eine Bewertung der gefundenen Schwachstellen in Form der potenziellen Risiken sowie Empfehlungen zur Kompensation der Schwachstellen bzw. der Risiken enthalten. Der Bericht muss in jedem Fall die Nachvollziehbarkeit der Tests und der dadurch offengelegten Schwachstellen garantieren. Die Feststellungen und die daraus resultierenden Risiken für die IT-Sicherheit sollten nach Beendigung der Prüfungshandlungen in einem Abschlussgespräch ausführlich besprochen werden.

Quelle:

Studie „Durchführungskonzept für Penetrationstests“ des Bundesamts für Sicherheit in der Informationstechnik

Ansprechpartner: Jörg Wöhler (Leitender Berater)

Datenschutz – Literatur für die praktische Umsetzung

Definition, Gesetze und Richtlinien

Datenschutz, das ist per Definition der Schutz personenbezogener Daten vor Missbrauch.

Seit 1980 existieren mit den OECD Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data international gültige Richtlinien. Das Europäische Parlament und der Europäische Rat haben mit der Richtlinie 95/46/EG (Datenschutzrichtlinie) verbindliche Mindeststandards für den Datenschutz der europäischen Mitgliedsstaaten festgeschrieben. Auf Bundesebene regelt das Bundesdatenschutzgesetz (BDSG) den Datenschutz für die Bundesbehörden und den privaten Bereich (d. h. für alle Wirtschaftsunternehmen und Privatperson gegenüber Privatperson). Daneben gibt es Landesdatenschutzgesetze sowie weitere spezielle Regelungen zum Datenschutz.

Pflicht zur Benennung eines betrieblichen Datenschutzbeauftragten

Unternehmen haben einen betrieblichen Beauftragten für den Datenschutz (sog. betrieblicher Datenschutzbeauftragter/bDSB) dann schriftlich zu bestellen, wenn sie bei der automatisierten Datenverarbeitung mindestens 10 Personen oder bei Verarbeitung auf andere Weise mindestens 20 Personen beschäftigen. Unabhängig von der Anzahl der Arbeitnehmer haben nicht öffentliche Stellen einen bDSB zu bestellen, soweit sie automatisierte Verarbeitungen vornehmen, die wegen besonderer Sensitivität vor Einsatz zu prüfen sind (Vorabkontrolle) oder die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung oder der anonymisierten Übermittlung erheben, verarbeiten oder nutzen.¹

Relevanz der „8 Gebote des Datenschutzes“ für die IT

Aus Sicht der IT hat § 9 BDSG die höchste Relevanz, wonach technische und organisatorische Maßnahmen zu treffen sind, um die Ausführungen des Gesetzes zu gewährleisten. Was konkret gefordert wird, spezifizieren zunächst einmal die Kontrollziele in der Anlage zu § 9 S. 1 BDSG, die so genannten „8 Gebote des Datenschutzes“. Danach sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind,

1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),
2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),
3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),
4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),
5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),

¹ 1. §§ 4f und 4g BDSG; 2. Erstes Gesetz zum Abbau bürokratischer Hemmnisse am 26. August 2006

AKTUELLES

6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),
7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),
8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. (Zweckbestimmung²)

Die Umsetzung dieser Datenschutzziele dient auch der IT-Sicherheit und schafft somit eine große Schnittmenge und Abhängigkeit voneinander. Für den Datenschutz stellen die Maßnahmen der IT-Sicherheit ein wesentliches Werkzeug dar, um seine Ziele zu erreichen. Umgekehrt betrachtet die IT-Sicherheit den Datenschutz bei der Verarbeitung personenbezogener Daten als eine wesentliche Quelle für umzusetzende Anforderungen.

Literaturhinweise für die praktische Umsetzung

Fraglich ist nun, welche konkreten Bereiche der IT betroffen sind, welche Maßnahmen es umzusetzen gilt und vor allem: Wo gibt es hierzu weitergehende Informationen?

Eine wesentliche Literaturquelle ist der „Baustein 1.5 - Datenschutz“ der IT Grundschutzkataloge des BSI³. Dieses 58-seitige Dokument erläutert hinreichend ausführlich die Vorschriften des BDSG und die wesentlichen Gefährdungen i. S. v. Risiken. Außerdem wird ein Maßnahmenbündel mit konkreten Handlungsempfehlungen vorgestellt, das für IT-Systeme und -Prozesse in Bezug auf Datenschutz umgesetzt werden sollte. Die Empfehlungen beziehen sich auf Planung und Konzeption, Umsetzung sowie Betrieb. Darüber hinaus steht mit Anlage „Formular zu Baustein B 1.5 Datenschutz“ eine praktische Checkliste zur Verfügung.

Für Unternehmen, die SAP im Einsatz haben, steht mit dem 124-seitigen „Leitfaden Datenschutz für SAP ERP 6.0“ vom 30.05.2008 der DSAG e. V.⁴ ein umfassendes Handwerkszeug zur Verfügung. Dieser gibt Anhaltspunkte für die Vorgehensweise bei der Umsetzung der Anforderungen der Datenschutzvorschriften bei Einsatz der SAP-Software. Der Leitfaden Datenschutz behandelt Fragestellungen, die bereits in den SAP-Sicherheitsleitfäden oder in anderen Prüfleitfäden des DSAG AK-Revision enthalten sind, mit Fokus auf datenschutzrechtliche Aspekte. Hervorzuheben ist, dass z. T. auch auf modulspezifische Besonderheiten, z. B. HCM (Human Capital Management), eingegangen wird. Da SAP ERP als international eingesetzte Standardsoftware konzipiert ist, berücksichtigt der Leitfaden neben der deutschen Datenschutzgesetzgebung auch die o. g. EU-Richtlinie 95/46/EG.

Literatur Quellen mit Hyperlink:

- [OECD - Guidelines on the Protection of Privacy and Transborder Flows of Personal Data](#)
- [BDSG - Bundesdatenschutzgesetz](#)
- [EU-Richtlinie 95/46/EG](#)
- [BSI - Baustein 1.5 - Datenschutz](#)
- [DSAG e. V. - Leitfaden Datenschutz für SAP ERP 6.0](#)

Ansprechpartner: Jörg Wöhler (Leitender Berater)

² Redaktionelle Anmerkung

³ BSI = Bundesamt für Sicherheit in der Informationstechnik

⁴ DSAG e.V. = Deutsche SAP Anwendergruppe e. V.

Der „Dreiklang“ von Revision, Risikomanagement und Compliance

Abgrenzungen und notwendige Zusammenarbeit

Neben der klassischen Organisationseinteilung eines Unternehmens in Stabs- und operative Abteilungen und der davon abgeleiteten Leitungsebene, wie Leiter der Rechtsabteilung, Leiter der Revisionsabteilung, Leiter der Marketingabteilung bzw. den entsprechenden englischen Bezeichnungen, haben sich spezialisierte – rechtlich verankerte – Funktionen nach dem Revisionschef ergeben, wie:

- Riskmanager
- Compliance Officer
- Geldwäschebeauftragter
- Sicherheitsbeauftragter
- Gleichstellungsbeauftragter
- und andere mehr.

Bei einem ersten Einordnungsversuch dieser neuen Funktionsträger in die Organisationsstruktur der Unternehmen stellt man fest, dass die Funktionsträger zwar im Organigramm einer Abteilung zugeordnet werden können, die Funktionen selber aber abteilungsübergreifend ausgeübt werden und entsprechende Informationsstränge eingerichtet werden müssen.

Weiter war und ist es im Unternehmen gewöhnungsbedürftig, dass ein Teil dieser Funktionsträger zwar nach dem Direktionsrecht hierarchisch eingebunden ist, die Träger ihre Funktionen jedoch unabhängig ausüben sollen und notwendige Kompetenzen für die abteilungsübergreifende unabhängig auszuübenden Funktionen im Rahmen gesetzlicher Bestimmungen als personell übertragene Geschäftsführungskompetenzen „verliehen“ werden.

Daraus entstehen wiederum Berichtspflichten, die auf dem Wege zur Geschäftsführung nicht durch die Hierarchie korrigierbar oder veränderbar sind.

Soweit entsprechende Organisationsregelungen gesetzlich getroffen werden, verändern sich die hergebrachten Corporate Governance Vorstellungen gesellschaftsrechtlich und letztlich haftungsrechtlich erheblich.

Für die Unternehmen ist u. a. bedeutsam, welche Verbindungsstrukturen abteilungsübergreifend und hierarchisch neu geordnet werden müssen und inwieweit mit welchen Folgen auch hier der Gesetzgeber eingreift.

In der Diskussion sind insbesondere die Abgrenzung einerseits und die Zusammenarbeit andererseits zwischen Riskmanagement, Compliance und Revision. Dies ist im Sektor der Finanzdienstleistungsinstitute am stärksten geregelt, betriebswirtschaftlich organisiert und in der praktischen Erprobung auf dem Wege zur allgemeinen Akzeptanz.

Über die Umsetzung europäischer Richtlinien wird dieser „Dreiklang“ mehr und mehr auf andere Sektoren übertragen und über betriebswirtschaftliche Einsicht und Rechtsprechung als Grundsatz einer allgemein ordnungsgemäßen Geschäftsführung verstanden.

Über die organisatorischen Einheiten der drei Funktionen gibt es jeweils für sich genommen umfangreiche betriebswirtschaftliche und rechtliche Literatur. Deshalb sollen hier nur die für den „Dreiklang“ spezifischen Faktoren hervorgehoben werden.

An der herkömmlich besonderen Stellung des Revisionsleiters haben sich die anderen Einheiten ausgerichtet:

AKTUELLES

Der Revisionsleiter (die Revision) hat eine herausgehobene Stellung, ist in seinen Funktionen im Rahmen des Direktionsrechts in gewissen Grenzen unabhängig, revidiert Tätigkeiten außerhalb seines Zuständigkeitsbereiches und berichtet direkt an den Vorstand. Im Rahmen des Jahresabschlusses greift der Wirtschaftsprüfer auf seine Ergebnisse zurück und kontrolliert die Ordnungsmäßigkeit seiner Revisionstätigkeit. Daneben wird im Rahmen verbindlicher Quality Assessments die Funktionsfähigkeit der Internen Revision und die Einhaltung der Standards des DIIR überprüft.

Weitergehende Standards aus dem Banken- und Versicherungsumfeld geben Pflichtprüfungen, die organisatorische Eingliederung und Prüfungsturnus vor. Außerdem ist die Ausgestaltung der Revisionsfunktion durch die Mindestanforderungen für das Risikomanagement (Banken und Versicherungen) vorgegeben worden.

Der Aufsichtsrat oder ein Prüfungsausschuss kann die Revisionsberichte (über den Vorstand) anfordern oder auch direkt auf die Interne Revision zugehen.

Die Revision prüft **alle Vorgänge** im Unternehmen und auditiert die **Geschäftstätigkeit sowohl nachträglich als auch ex-ante (projektbegleitend)** auf ihre Ordnungsmäßigkeit, Wirtschaftlichkeit, Sicherheit etc.

Sie wird hierbei unter Compliance Gesichtspunkten immer stärker zum Berater von Vorstand und Führungskräften in dem sie regelmäßig Kontroll- und Risikomanagementsysteme auf ihre Wirksamkeit und Angemessenheit beurteilt, bei der Aufklärung von Verstößen und Delikten mitwirkt sowie ein Qualitätsurteil über die Compliance Organisation (Assurance) abgibt.

Der Vorstand hat für die Einhaltung der gesetzlichen Bestimmungen und der unternehmensinternen Richtlinien zu sorgen und wirkt auf deren Beachtung durch die (Konzern)-Unternehmen hin (Deutscher Corporate Governance Kodex). Corporate Compliance steht somit für rechtskonformes Verhalten durch organisatorische und ablauftechnische Vorkehrungen, Verfahren und Funktionen. Die praktische Überwachung erfolgt in der **Compliance-Stelle, geleitet vom Compliance Officer**, der das rechtmäßige den gesetzlichen und innerbetrieblichen Regeln entsprechende Handeln des Unternehmens sicherstellt.

Der Compliance Officer berät die Geschäftsleitung im Vorfeld von Geschäften, wirkt bei der Aufstellung von Regelwerken mit und verfolgt die Geschäftshandlungen während ihres Ablaufs auf rechtliche Interessenkonflikte mit den Kunden oder auch innerhalb des Unternehmens.

Der Wunsch nach effizienten Prozessen und angemessenen Erträgen steht teilweise in einem diametralen Spannungsfeld zum Umfang an vorhandenen externen Anforderungen und Einhaltung von Vorschriften. Die Herausforderung besteht darin eine Ressourcen schonende aber dennoch effektive Compliance-Organisation zu implementieren.

Im Finanzdienstleistungsbereich ist die Stellung der Compliance Organisation gesetzlich gestärkt, seine funktionelle Unabhängigkeit besonders betont und sowohl sein Aufgabenfeld wie seine organisatorische Einbindung weitestgehend vorgegeben. Innerbetrieblich besteht eine Vortragspflicht sowohl gegenüber dem Vorstand als auch gegenüber dem Aufsichtsrat. Er ist offizielle Ansprechstelle der zuständigen Aufsichtsbehörde, ist ihr gegenüber aber nicht am Vorstand vorbei berichtspflichtig.

Der Wirtschaftsprüfer hat die Funktionsfähigkeit und Effektivität seines Handelns zu bestätigen.

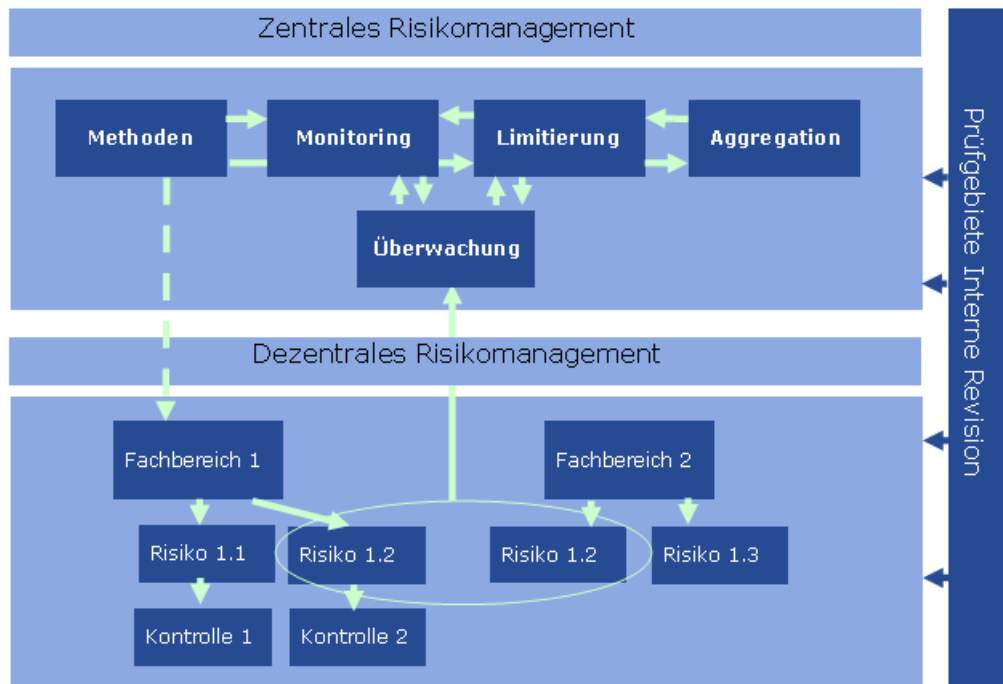
Das **Risikomanagement** hat die wirtschaftlich finanzielle Existenzfähigkeit des Unternehmens sicherzustellen. Ihm obliegt die individuelle und branchenspezifische Risikoidentifikation und -bewertung, sowie die Mitwirkung bei der Entwicklung der Geschäftsstrategie über die dauerhafte Prüfung der Risikotragfähigkeit bis zur Kontrolle der Planerreicherung.

Im Rahmen der Risikosteuerung kann das Risikomanagement Grenzen- und Rahmendaten für einzelne Geschäftsfelder vergeben, um die letztlich vom Vorstand zu verantwortenden strategischen Vorgaben und Risikoentscheidungen sicherzustellen. Das Risikomanagement ist den Unternehmen im Finanzsektor ausschließlich und unter Berücksichtigung der Absicherung der

AKTUELLES

Marktfunktionalität gesetzlich vorgegeben und von der Aufsichtsbehörde im Einzelnen verbindlich ausgestaltet worden.

Vor dem Hintergrund der MaRisk (VA) ist in diesem Zusammenhang auch die Beurteilung und Verbindung von zentralem und dezentralem Risikomanagement von erheblicher Bedeutung. Hiernach sind zur Sicherstellung der Funktionsfähigkeit sämtlicher Bestandteile des Risikomanagementsystems dem Risiko entsprechende Kontrollen einzurichten.



Gesellschaftsrechtlich wird es den Verpflichtungen einer ordnungsgemäßen Geschäftsführung zugeordnet. Im Aufsichtsrat muss über die Zusammensetzung der Mitglieder das Verständnis für das Risikomanagement und die Prüfung der Funktionsfähigkeit sichergestellt sein.

Fasst man die Definition des Risikomanagements als zusammenfassende Geschäftsführungsverpflichtung sehr weit, umfasst Risikomanagement als Steuerung des wirtschaftlichen-, finanziellen-, rechtlichen- und Reputationsrisikos auch Compliance und Revision.

Hieraus resultiert die Vorstellung, man könne doch alle diese Tätigkeiten in einer Abteilung operationell zusammenfassen; also etwa der schon bestehenden Revisionsabteilung Compliance und Risikomanagement oder dem Risikomanagement Revision und Compliance zuordnen. Dies ist unterhalb der umfassenden Verantwortung der Geschäftsführung jedoch mit Ausnahme sehr kleiner Unternehmen nicht möglich. Auch widersprechen aufsichtsrechtliche Regelungen zur Funktionstrennung diesem Ansinnen. Die Kompetenzen müssen von der Geschäftsführung getrennt delegiert werden. Die Prüfung der Revision umfasst auch die Ordnungsmäßigkeit des Risikomanagements und der Compliance-Stelle; Compliance relevante Interessenkonflikte, z. B. Insidergeschäfte, können auch von Angestellten der Revisionsabteilung und des Konfliktmanagements getätigt werden.

Die getrennten Verantwortungen können nur effektiv ohne Überschneidungen und Doppelarbeiten wahrgenommen werden, wenn sie aufeinander abgestimmt sind.

AKTUELLES

Einige Beispiele:

Das Risikomanagement gibt in einem Handelsbereich im Einzelfall Risikobegrenzungen vor. Veränderungen der Geschäftsvolumina können von der Compliance-Stelle jedoch nur schwer als Überschreitung eines vorgegebenen Rahmens definiert werden, wenn sie nicht die Vorgaben des Risikomanagements kennt.

Verstöße gegen betriebsinterne Regelungen der Compliance-Stelle, etwa Mitarbeitergeschäfte in bestimmten Wertpapieren zuzulassen, werden nachträglich von der Revisionsabteilung aufgedeckt. Die Revisionsabteilung stellt fest, dass Informationsverpflichtungen der Marktabteilung gegenüber der Compliance-Stelle nicht eingehalten werden. Die Compliance-Stelle entdeckt, dass die Datenversorgung über Mitarbeitergeschäfte aufgrund von Systembrüchen oder Datenintegritäten unvollständig ist und informiert die Revision hierüber. Die Revision berücksichtigt die Informationen bei der Revisionsplanung oder lässt diese in aktuelle Prüfungen einfließen.

Die vielfachen Schnittstellen der drei Abteilungen müssen definiert werden. Die Entscheidungen der Funktionsträger müssen im Rahmen notwendiger und definierter Vertraulichkeitsregelungen den anderen Funktionsträgern bekannt sein. Prüfungstätigkeiten von Compliance und Revision in den Marktabteilungen müssen aufeinander abgestimmt sein. Feststellungen von Unregelmäßigkeiten können drohende Reputationsrisiken anzeigen.

Die Datensicherheit wie die Zugriffsmöglichkeiten auf denselben Datenpool sind wichtige Voraussetzungen für die erfolgreiche Arbeit der drei Funktionsstellen.

Compliance benötigt aktuelle Informationen aus allen Bereichen. Ein entsprechendes Meldewesen muss eingerichtet werden. Das Risikomanagement benötigt dieselben oder ähnliche Daten zur Risikokontrolle und die Revision muss bei Prüfungen auf aktuelle und akkurate Information und Dokumente zugreifen können.

Leider gibt es Hinweise, dass zum Nachteil der Unternehmen die Zusammenarbeit der drei Funktionen nicht immer optimal aufeinander abgestimmt ist oder bei der Implementierung neuer Regelungen vernachlässigt wurde. Im Finanzsektor prüfen die Wirtschaftsprüfer im Auftrag der Aufsichtsbehörden, ob der Dreiklang von Risikomanagement, Compliance und Revision im Unternehmen nicht nur eingehalten, sondern auch „gelebt“ wird.

Die optimale Gestaltung ist wesentliche Geschäftsführungsaufgabe. Eine Vernachlässigung oder möglicherweise aus Kostengründen gefundene Vereinfachung kann sich zum Nachteil des Unternehmens entwickeln.

Im Finanzsektor hat die Aufarbeitung der Krise gezeigt, dass dem Risikomanagement im weiteren Sinne erhöhte Aufmerksamkeit gewidmet werden muss. Für Risikomanagement, Compliance und Revision und deren Zusammenwirken werden aktuell neue Regelungen entwickelt, die die geschilderten Grundsätze verfeinern oder erweitern werden. Andere Wirtschaftssektoren werden erfasst oder entwickeln im Eigeninteresse ähnliche Konstruktionen.

Ansprechpartner: Dr. Jürgen Brockhausen (BROCKHAUSEN Beratung und Compliance GmbH) und Christof Merz (Geschäftsbereichsleiter, agens Consulting)

AKTUELLES

Rückblick auf die Seminare am 30.09. und 01.10.09 in Düsseldorf

„Fraud-Präventionsmaßnahmen nach erfolgter Risiko- und Gefährdungsanalyse“ sowie „Juristische Grundlagen für das Fraud-Management“

Am 30. September wurde die Fraud-Veranstaltungsreihe in Düsseldorf mit dem Thema **„Fraud-Präventionsmaßnahmen nach erfolgter Risiko- und Gefährdungsanalyse“** fortgeführt. Das Seminar wurde durch die Herren Peter Zawilla, Geschäftsführer der FMS Fraud Management and Services GmbH sowie Henning Tenzer, Leitender Berater der agens Consulting GmbH, durchgeführt:



Referenten v.l.: Peter Zawilla, Geschäftsführer der FMS Fraud Management and Services GmbH und Henning Tenzer, agens

Die Erfahrungen der Vortragenden trugen zur hohen Anschaulichkeit und Praxisnähe des vermittelten Lernstoffes bei. Zur Zielerreichung wurden mit den neun Teilnehmerinnen und Teilnehmern folgende Schwerpunkte erarbeitet:

- „Know your Risks“: Das Kennen von Gefährdungspotenzialen und möglichen Risiken als wesentliche Voraussetzung für die Implementierung angemessener risikominimierender Maßnahmen sowie zur optimalen Gestaltung der Geschäftsprozesse
- Erstellung bzw. Durchführung von Gefährdungsanalysen: Empfehlungen zur praktischen Vorgehensweise
- Motivlagen von Mitarbeitern und externen Personen für Manipulationen und dolose Handlungen
- Indizien („Red Flags“) für Delikt-/Schadensfälle (sach-/engagementbezogen, mitarbeiterverhaltensbezogen sowie im Verhalten von Kunden, Lieferanten und Vermittlern) anhand von konkreten Praxisfällen
- Tragende Säulen und wesentliche Voraussetzungen für ein wirksames und „gelebtes“ IKS eines Unternehmens
- Praxisorientierte Optimierungsmöglichkeiten für das IKS
- Bausteine effizienter und nachhaltiger Mitarbeitersensibilisierung
- Sensibilisierung für Auffälligkeiten durch konsequente Aus- und Weiterbildung der Mitarbeiter

Am folgenden Tag ging die Reihe auch schon weiter: **„Juristische Grundlagen für das Fraud-Management“** stand auf dem Programm.

AKTUELLES

Das Seminar wurde durch Herrn Peter Zawilla, Geschäftsführer der FMS Fraud Management and Services GmbH sowie die Rechtsanwälte Dr. Heiner Hugger, Dr. Michael Kremer und Dr. Peter Christ der Anwaltssozietät Clifford Chance, durchgeführt.

In der Veranstaltung wurde das rechtlichen Grundwissens zur Bekämpfung von dolosen Handlungen zum Nachteil von Unternehmen sowie Praxistipps zur Zusammenarbeit mit den Strafverfolgungsbehörden und zur Durchsetzung zivilrechtlicher Ansprüche vermittelt.



Dr. Peter Christ, Rechtsanwalt der internationalen Anwaltssozietät Clifford Chance

Die Teilnehmer haben insbesondere die verständliche Vermittlung des komplexen juristischen Wissens für den Nichtjuristen geschätzt.

Beide Seminare wurden durch die Teilnehmer als wertvoll und gut gelungen beurteilt.

Am 13.07.10 sowie 14. – 15.07.10 wiederholen wir zwei Fraud-Specials in Köln:

13.07.10: „Fraud-Präventionsmaßnahmen nach erfolgter Risiko- und Gefährdungsanalyse“

Weitere Informationen:

http://www.agens.com/de/Unternehmen/Publikationen_und_News/News/2009/fraud_13_072010.php

14. – 15.07.10: „Fraud-Sonderuntersuchungen und Deliktrevisionen“

Weitere Informationen:

http://www.agens.com/de/Unternehmen/Publikationen_und_News/News/2009/fraud_14_15072010.php

Darüber hinaus bieten wir in schon gewohnter Weise unsere Fraud-Prevention-Tagesveranstaltung als Erfahrungsaustausch unabhängig von der Seminarreihe an:

23.02.10 Hannover: „Prävention von wirtschaftskriminellen Handlungen - Aktuelles, Trends und Praxisbeiträge“

Weitere Informationen:

http://www.agens.com/de/Unternehmen/Publikationen_und_News/News/2009/fraud_2_3022010.php

Wir freuen uns über Ihre Teilnahme!

Ansprechpartner: Doris Jeska (Assistentin Vertrieb)

AKTUELLES

Compliance Symposium 24. und 25. Februar 2010 in Hannover

Ganzheitliche Risk Assurance mit Grundsätzen guter Unternehmensführung - Lehren aus der Finanzkrise -

Gemeinsam mit der Brockhausen Beratung & Compliance GmbH führte agens im Februar 2009 sehr erfolgreich das erste Compliance Symposium durch. Im Februar 2010 wird es nun eine Folgeveranstaltung unter dem Titel „Ganzheitliche Risk Assurance mit Grundsätzen guter Unternehmensführung - Lehren aus der Finanzkrise - geben.



Veranstaltungsort: Hotel Mercure Hannover City

In der jüngsten Vergangenheit haben die Fälle von Korruption, Bestechung und sonstige für die betroffenen Unternehmen in der Außendarstellung negativen Handlungen enorm zugenommen. Illegale bzw. schädliche Handlungen lassen sich nicht allein mit Gesetzen und dichten Kontrollsystemen verhindern.

Eine starke Compliance-Organisation und ein gut funktionierendes Internes Kontrollsystem (IKS) minimieren oder verhindern mögliche Schäden und reduzieren negative Folgen für die Reputation des Unternehmens.

Das gemeinsame Ziel liegt daher neben der klassischen Sicherstellung der Rechtskonformität aller Handlungen auch darin, Korruption und Manipulation zu verhindern, die Loyalität von Management und Mitarbeitern durch ein Wertemanagement zu stärken und die Unternehmensreputation zu steigern.

In diesem Zusammenhang stellt sich auch die Frage, ob eine starke Compliance-Organisation und Wertemanagement Wege aus der derzeitigen Finanzkrise aufzeigen bzw. unterstützen können.

Das Compliance Symposium bietet Ihnen einen Überblick über Ansätze und Methoden zur Umsetzung einer Compliance-Organisation, Durchführung von Schwachstellenanalyse und die Weiterentwicklung der rechtlichen Anforderungen.

Neben der praktischen Ausgestaltung eines IKS anhand von Beispielen wird auch viel Raum zum Erfahrungsaustausch und aktiven Diskussionen geboten.

Weitere Hintergrundinformationen zur Veranstaltung sowie das Anmeldeformular finden Sie hier:

http://www.agens.com/de/Unternehmen/Publikationen_und_News/News/2009/compliance_for_um_hannover2010.php

Über Ihre Teilnahme freuen wir uns!

Ansprechpartner: Doris Jeska (Assistentin Vertrieb)

AKTUELLES

Auswertung der Online-Umfrage

Zum Thema „Wissensmanagement im Unternehmen am Beispiel Interner Revisoren“

Im Rahmen der empirischen Studie wurde untersucht, wie sich das aktuelle Wissensmanagement in Revisionsabteilungen gestaltet.

Die Ergebnisse der online-Befragung liegen nun vor und wir würden sie Ihnen sehr gern

**am 13. November 2009
von 10:00 bis 12:00 Uhr
in den Räumen der agens in Ellerau**

präsentieren. Kosten entstehen Ihnen für die Teilnahme seitens agens nicht.

Bitte melden Sie Ihre Teilnahme bis spätestens 30.10.2009 unter Mail akg-vws@agens.com oder telefonisch unter 04106 7777 0 unter dem Stichwort „Präsentation Wissensmanagement“ an. Nennen Sie uns bitte Ihre Mailadresse und Telefonnummer sowie die Namen der teilnehmenden Personen.

Herzlichen Dank nochmals an alle Teilnehmer der Studie für Ihre Unterstützung!

Ansprechpartner: Dr. Peter Wesel (Peter.Wesel@agens.com) (Senior Berater)

AKTUELLES

agens Risk Manager als Web Anwendung

In unserem neuen webbasierten agens Risk Manager haben wir alle Funktionalitäten eines modernen Risikomanagementsystems für Finanzdienstleister und Versicherungen in Anlehnung an die MaRisk abgebildet. Das System enthält alle notwendigen Komponenten wie Risikoanalyse, Risikoquantifizierung und Frühwarnfunktionalität, Risikotragfähigkeitsberechnung sowie Berichtswesen.

In das Tool sind unsere Erfahrungen und das Methoden Know-how aus zahlreichen Projekten eingeflossen.

Das modulare Design des Systems erlaubt es, Erweiterungen jederzeit schnell und unkompliziert ins System zu integrieren.

Das System ist plattformunabhängig als Server- oder Client Version verfügbar und kann durch die vorhandene Mehrsprachigkeit international eingesetzt werden.



Der neue webbasierte agens Risk Manager ist fachlich und technisch für die Zukunft gerüstet. Überzeugen Sie sich von den Vorteilen des neuen agens Risk Manager. Reduzieren Sie Ihre Kosten und nutzen Sie alle Vorteile eines modernen und zeitgerechten Risikomanagementsystems.

Sollten wir Ihr Interesse geweckt haben, schalten wir Ihnen gern einen Testzugang frei. Bei Interesse senden Sie uns einfach eine E-Mail:

jan-hendrik.uhlenberg@agens.com

Ansprechpartner Jan-Hendrik Uhlenberg (Senior Berater)



Literatur



IT-Revision in der Praxis

Klaus Schmidt, Dirk Brand
 ISBN-10: 3446417060
[\(Mehr ...\)](#)



Risikomanagement

Reinhard Alves
 ISBN-10: 3527504273
[\(Mehr ...\)](#)



Rechnungslegung, Steuerung und Überwachung von Unternehmen

Aktuelle Entwicklungen, Krisenbewältigungen und Reformbestrebungen
 Carl-Christian Freidank
 ISBN-10: 3503116494
[\(Mehr ...\)](#)



Revision des Rechnungswesens

Arbeitskreis „Revision d. Finanz- u. Rechnungswesens“ d. DIIR
 ISBN-10: 3503058907
[\(Mehr ...\)](#)



MaRisk für Kreditgenossenschaften

Interpretation und praktische Umsetzungshilfen
 Genossenschaftsverband e.V. (Hrsg.)
 ISBN-10: 3871511226
[\(Mehr ...\)](#)



Handbuch Interne Kontrollsysteme (IKS)

Oliver Bungartz
 ISBN-10: 3503114734
[\(Mehr ...\)](#)



Neuausrichtung der Versicherungsaufsicht (Solvency II)

Marion Rittmann von Gabler
 ISBN-10: 3834920401
[\(Mehr ...\)](#)



Query-Reporting mit SAP ERP

Stephan Kaleske
 ISBN-10: 3836214334
[\(Mehr ...\)](#)

SEMINARTERMINE

Im Folgenden möchten wir Ihnen wieder ausgewählte Seminare des agens Revisionsteams vorstellen.

November bis Dezember 2009

Fraud nachhaltig vermeiden - DIIR (Mehr...)	02. – 03.11.2009
Einführung in die Interne Revision - DIIR (Mehr...)	02. – 05.11.2009
Einführung in die IT-Revision - DIIR (Mehr...)	02. – 05.11.2009
Aufbau in die Interne Revision im Unternehmen - DIIR (Mehr...)	05. – 06.11.2009
Die 10 „S“ für Revisionsleiter - Modul 6: Steuerung durch den Revisionsleiter - DIIR (Mehr...)	10.11.2009
Berichterstattung der Internen Revision - DIIR (Mehr...)	16. – 18.11.2009
Grundlagen der Führungswirkungsprüfung - DIIR (Mehr...)	30.11. – 01.12.2009
Sicherheit im Internet – Prüfung neuer Informationstechnologien - DIIR (Mehr...)	30.11. – 02.12.2009
Prüfung der Wirtschaftlichkeit von Geschäftsprozessen - DIIR (Mehr...)	30.11. – 03.12.2009
Projekte prüfen aus Sicht der Internen Revision - DIIR (Mehr...)	02. – 04.12.2009
CobIT-Workshop - DIIR (Mehr...)	03. – 04.12.2009
Wirtschaftlichen Einsatz der IT prüfen - DIIR (Mehr...)	07. – 08.12.2009
Interne Kontrollsysteme prüfen und gestalten (IKS I) - DIIR (Mehr...)	07. – 09.12.2009
Einführung in die Interne Revision - DIIR (Mehr...)	07. – 09.12.2009
Immobilienaudit – Haub + Partner (Mehr...)	10.12.2009
Der Revisionsbericht – Teil 2 – Haub + Partner (Mehr...)	14. – 15.12.2009

Spezielle Seminare für den öffentlichen Dienst und die EU-Finanzkontrolle von November bis Dezember 2009

Datenanalyse mit modernen Prüfwerkzeugen – agens (Mehr...)	11. – 13.11.2009
Gesprächs- und Verhandlungstechniken für Prüfende - agens (Mehr...)	23. – 25.11.2009
Workshop: Risikoorientierte Prüfungsplanung – agens (Mehr...)	26.11.2009
Workshop: Qualitätsmanagement für die EU-Finanzkontrolle – agens (Mehr...)	30.11.2009

Ansprechpartner: Dr. Peter Wesel (Senior Berater)

MICROSOFT EXCEL

Microsoft Excel

Auch wenn Microsoft Excel ein weit verbreitetes Standardprodukt in vielen Unternehmen ist, bleiben jede Menge Funktionen im Alltag verborgen. Wir möchten an dieser Stelle Hilfeleistung bieten und Ihnen regelmäßig über ausgewählte Funktionen/Formeln berichten.

Funktion: Aufgelaufene Zinsen eines Wertpapiers (AUFGELZINSF)

Das Funktion „AUFGELZINSF“ liefert die aufgelaufenen Zinsen (Stückzinsen) eines Wertpapiers, die bei Fälligkeit ausgezahlt werden. Die Funktion dient dazu, den Tageswert von festverzinslichen Papieren zu kalkulieren.

Die aufgelaufenen Zinsen eines Wertpapiers kann man anhand folgender Formel berechnen:

$$\text{Aufgelaufene Zinsen} = \text{Kurz} * \text{Zins} * \frac{A}{D}$$

Dabei gilt:

A = Anzahl der aufgelaufenen Tage, die entsprechend einer monatlichen Basis gezählt werden. Für Zinsen bei Tilgungsraten wird die Anzahl an Tagen ab dem Emissionstermin bis zum Fälligkeitstermin verwendet;

D = Jährliche Jahresbasis.

Man kann auch sehr schnell die aufgelaufenen Zinsen eines Wertpapiers in Excel unter der Anwendung der finanzmathematischen Funktion „AUFGELZINSF“ ermitteln.

Beispiel für die Ermittlung der aufgelaufenen Zinsen eines Wertpapiers

Ein Investor hat am 01.01.2009 die festverzinslichen Wertpapiere im Wert von 10.000 EURO erworben, die am 30.06.2009 fällig sind. Der jährliche Kuponzinssatz des Wertpapiers beträgt 10 %. Man muss die aufgelaufenen Zinsen zum 30.06.2009 ermitteln.

Lösung:

Für die Ermittlung der aufgelaufenen Zinsen verwendet man die finanzmathematische Funktion „AUFGELZINSF“.

Menüleiste: Einfügen -> Funktion... -> Kategorie auswählen: Finanzmathematik -> Funktion auswählen: AUFGELZINSF -> OK.

Im erschienenen „Assistent“ werden die folgenden Daten per Mausklick aus der Tabelle eingegeben:

- In der Zeile „Emission“ wird das Datum der Ausgabe des Wertpapiers (Zelle C4) eingetragen. Ab diesem Termin wird das Papier verzinst.
- In der Zeile „Abrechnung“ wird der Fälligkeitstermin (Zelle C5) eingetragen;
- In der Zeile „Nominalzins“ wird der Kuponzinssatz (Zelle C6) eingetragen;
- In der Zeile „Nennwert“ wird der Nennwert des Wertpapiers (Zelle C7) eingetragen;
- In der Zeile „Basis“ wird angegeben, auf welcher Basis (Zelle C8) die Zinstage gezählt werden.

Basis	Basis für die Zählung der Tage
0 oder nicht angegeben	USA (NASD) 30/360
1	Taggenau/taggenau
2	Taggenau/360
3	Taggenau/365
4	Europa 30/360

- Um den Assistent zu beenden, drückt man auf „Ok“.

Der ergebende Betrag sind die aufgelaufenen Zinsen zum 30.06.2009.

MICROSOFT EXCEL

Syntax:

AUFGELZINSF(Emission;Abrechnung;Nominalzins;Nennwert;Basis)

- **Emission:** ist das Datum der Wertpapieremission
- **Abrechnung:** ist der Fälligkeitstermin des Wertpapiers
- **Nominalzins:** ist der jährliche Nominalzins (Kuponzinssatz) des Wertpapiers
- **Nennwert:** ist der Nennwert des Wertpapiers. Wenn Sie keinen Nennwert angeben, verwendet AUFGELZINSF den Wert 1.000 €
- **Basis:** gibt an, auf welcher Basis die Zinstage gezählt werden

Hinweise:

- Datumsangaben werden in Microsoft Excel als fortlaufende Zahlen gespeichert, damit sie für Berechnungen verwendet werden können. Standardmäßig ist der 1. Januar 1900 die fortlaufende Zahl 1 und der 1. Januar 2008 die fortlaufende Zahl 39448, da dieses Datum 39448 Tage nach dem 01.01.1900 liegt. Microsoft Excel für den Macintosh verwendet als Standard ein anderes Datumssystem.
- Emission, Abrechnung und Basis werden zu ganzen Zahlen gekürzt, indem ihre Nachkommastellen abgeschnitten werden.
- Ist Emission oder Abrechnung kein zulässiges Datum, gibt AUFGELZINSF den Fehlerwert #WERT! zurück.
- Ist Nominalzins ≤ 0 oder ist Nennwert ≤ 0 , gibt AUFGELZINSF den Fehlerwert #ZAHL! zurück.
- Ist Basis < 0 oder ist Basis > 4 , gibt AUFGELZINSF den Fehlerwert #ZAHL! zurück.
- Ist Emission = Abrechnung, AUFGELZINSF den Fehlerwert #ZAHL! zurück.

The screenshot shows an Excel spreadsheet with the following data:

Beschreibung	Daten
Emissionsdatum	01.01.2009
Fälligkeitstermin	30.06.2009
Kuponzinssatz	10%
Nennwert in EURO	10.000
Basis	3
Aufgelaufene Zinsen in EURO	493,15

The formula bar shows: `=AUFGELZINSF(C4;C5;C6;C7;C8)`

The 'Funktionsargumente' dialog box for AUFGELZINSF is open, showing the following arguments and their values:

Argument	Wert	Ergebnis
Emission	C4	= 39814
Abrechnung	C5	= 39994
Nominalzins	C6	= 0,1
Nennwert	C7	= 10000
Basis	C8	= 3

The dialog box also displays the result: `= 493,1506849` and the formula result: `Formelergebnis = 493,1506849`.

Ansprechpartner: Oleksandr Krasnopolskyy (Berater)

WHO IS WHO

In jeder Ausgabe werden wir Ihnen Mitglieder unseres Teams bzw. Mitarbeiter anderer Geschäftsbereiche, die uns bei Projekten unterstützen, vorstellen. Diesmal Ralph Rudolph, System-Administrator der agens Consulting GmbH:



Ralph Rudolph
System-Administrator

Welches war Ihr schönstes Musikerlebnis?

Ina Müller im Stadtpark Hamburg

Welche Freizeitaktivitäten üben Sie aus?

Freiwillige Feuerwehr, Schwimmen

Was hat Sie am meisten beeindruckt?

Das Miniaturwunderland in Hamburg

Was können Sie besonders gut kochen?

Chili Con Carne

Was beherrschen Sie im Haushalt besonders gut?

Fensterputzen

Was haben Sie als schönstes Käuferlebnis empfunden?

Grundstück

Was gefällt Ihnen an der agens am besten?

Die netten Kollegen

Was treibt Sie an?

Meine Frau

Welche Themen würden Sie gern beschleunigen?

Baugenehmigungsverfahren

Was sind Ihre persönlichen Motivationen?

Herausforderungen zu meistern

Wen bewundern Sie am meisten?

Alle Menschen, die sich ehrenamtlich für andere engagieren und alle, die kranke und pflegebedürftige Menschen betreuen

Was tun Sie, um sich zu entspannen?

Schwimmen, Spazierengehen

Wo hätten Sie gern Ihren Zweitwohnsitz?

An der Nordsee

Nennen Sie ein unentdecktes Traumreiseziel:

Kann ich nicht nennen, da noch unentdeckt

IMPRESSUM



agens Consulting GmbH
Buchenweg 11 - 13, 25479 Ellerau
Ein Unternehmen der [agens Gruppe](#)
HRB 3660 NO AG Kiel

Fon: +49(0)4106-7777-0
Fax: +49(0)4106-7777-333
Internet: <http://www.agens.com>
E-Mail: <mailto:info@agens.com>
Geschäftsführer (vertretungsberechtigt im Sinne § 6 EGG/§ 6 TDG):
Dr. Stefan Giesecke, Sven Jacob, Michael Kremsner
USt.-IDNr. : DE 176972447

Aktuelle Anzahl der Ausgaben (im Zwei-Monatsrhythmus): ca. 6.000

Zum Bestellen bzw. Abbestellen des „agens Audit & Risk Newsletters“ schicken Sie bitte eine E-Mail mit dem jeweiligen Betreff und Ihrem Namen an die folgende E-Mail Adresse:

rev-ace-newsletter-akte-pf@agens.com

Disclaimer

Alle Links zu externen Anbietern wurden zum Zeitpunkt ihrer Aufnahme auf ihre Richtigkeit überprüft. Da sich das Internet jederzeit wandelt, kann die agens Consulting GmbH nicht garantieren, dass diese Links zum Zeitpunkt des Besuchs a) noch zum Ziel führen oder b) noch dieselben Inhalte besitzen, wie zum Zeitpunkt der Aufnahme.

Insbesondere macht sich die agens Consulting GmbH nicht die Inhalte der Links zu Eigen und übernimmt dafür auch keine Verantwortung. Links zu externen Anbietern stellen keine Wertung oder eine Empfehlung der agens Consulting GmbH dar.

Der Inhalt dieses Newsletters ist urheberrechtlich geschützt. Ohne Genehmigung der agens Consulting GmbH darf der Inhalt dieser Seite in keiner Form reproduziert und/oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© agens Consulting GmbH, Ellerau, Deutschland, 2009. All rights reserved.

Stand: 25.Oktober 2009