

Dabei konnte die Vermutung der Buchhaltung, dass bei firmenübergreifenden Buchungen Doppelzahlungen entstehen, bestätigt werden (allerdings mit einem sehr geringen Anteil an den Gesamtzahlungen).

Fazit:

- Dieses Fallbeispiel zeigt, dass externe Prüfwerkzeuge auch ohne Programmieraufwand in der Lage sind, sehr flexible Auswertungen durchführen zu können. Durch die Fähigkeit, neue Abfrageparameter hinzuzufügen und bestehende Parameter durch »unscharfe« zu ersetzen, ergeben sich ganz neue Auswertungsmöglichkeiten, die dazu beitragen können, bisher nicht erkannte Doppelzahlungen zu identifizieren. Innerhalb von IDEA laufen die Auswertungen auch auf Standard-PCs schnell ab – auch bei über 600 000 Buchungen muss man selten mehr als ein paar Minuten warten.
- Voraussetzung dafür ist das Vorliegen der zu untersuchenden Daten im passenden Format. Bei IDEA lässt sich dieser Import aus einer Vielzahl von möglichen Formaten bewerkstelligen und sehr komfortabel mithilfe der Datensatzbeschreibung automatisieren. Auch bei den anschließenden Analysen lassen sich alle Aktionen als Makros aufzeichnen und jederzeit auf Knopfdruck wiederholen.
- Zeitintensiv ist vor allem das anschließende Nachvollziehen der auffälligen Belege über das IXOS-Archiv. Hier muss jeder Beleg manuell aufgerufen und kontrolliert werden, ob ein Storno oder Ähnliches nicht bereits durchgeführt wurde. Hier wäre eine direkt in SAP R/3 integrierte Prüfung sicherlich komfortabler.

- Von besonderer Wichtigkeit ist, aus der Vielzahl der Belege vor allem diejenigen herauszufinden, die eine sehr hohe Trefferwahrscheinlichkeit besitzen. Die hier vorgestellten Prüfungsalternativen haben gezeigt, dass je nach gewählten Parametern zwischen 64 und mehreren Tausend Datensätze zurückgeliefert werden.
- Grundsätzlich gibt es keinen Königsweg, an dessen Ende ausschließlich offene Doppelzahlungen stehen. Es ist bei der Auswahl der Daten ebenso wie bei der Parametrisierung der Abfrage immer abzuwiegen, wie hoch die Trefferquote sein soll und wie viele Belege im Zweifelsfalle zu untersuchen sind: Je »unschärfer« der Parameter, desto mehr potenzielle Doppelzahlungen kommen zum Vorschein, aber auch die Anzahl der Fehlalarme erhöht sich drastisch.

- Eine Prüfung durch ein externes Tool wie IDEA eignet sich aufgrund der leichten und schnellen Durchführung besonders um »mal mit den Daten zu spielen« und so eventuellen Prozessschwächen auf die Schliche zu kommen. Sollte eine Parameteranordnung als besonders sinnvoll erkannt werden, ist zu überlegen, ob eine entsprechende Prüfung nicht in Form eines Berichts in SAP direkt implementiert werden sollte, um den Weg »Export → Import → Analyse → Recherche« deutlich abzukürzen.

Dipl.-Kfm. Thorsten Kuznik leitet den Bereich Konzernrevision & Riskmanagement bei der DOUGLAS HOLDING AG seit 2000. Zuvor war Herr Kuznik in leitenden Funktionen in der Immobilienwirtschaft und in der Getränkeindustrie tätig.

Dipl.-Ökonomin Karla Engels gehört der Konzernrevision der DOUGLAS HOLDING AG seit 2001 an. Frau Engels verantwortet die dortige kfm. Revision und war zuvor fünf Jahre im Rechnungswesen der zuständigen Dienstleistungsgesellschaft der DOUGLAS-Gruppe tätig.

Dipl.-Kfm./BA Economics Ralf Hluchy, seit 2006 in der Konzernrevision bei der DOUGLAS HOLDING AG, obliegt die dortige IT-Revision. Schwerpunkte sind IT-bezogene System- und Prozessprüfungen, unter anderem mit Hilfe der Prüfsoftware IDEA. Zuvor war Herr Hluchy fünf Jahre als Projektleiter in der IT-Gesellschaft der DOUGLAS-Gruppe tätig.



Prof. Dr. Reinhard Vossbein*

IT-Security-Revision und IT-Security-Controlling

Inhalt

- 1 Vorbemerkung
- 2 Der IT-Security-Prozess
- 3 Zusammenhang zwischen IT-Security und Geschäftsprozessen
- 4 Geschäftsprozesse und interne Ordnungsmäßigkeitsvorgaben
- 5 Controlling und Kontrolle

1 Vorbemerkung

Unternehmen sind vom reibungslosen Betrieb ihrer die Geschäftsprozesse unterstützenden IT-Systeme abhängig. Ein zentraler interner Erfolgsfaktor ist die organisatorische Abwicklung der Geschäftsprozesse. Sie bezieht sich bei der heutigen Abhängigkeit der Unternehmen vom ordnungsgemäßen Betrieb ihrer IT auf die mit Hilfe geeigneter IT-Projekte umzusetzenden und zu optimierenden Geschäftsprozesse und Geschäftsmodelle des Unternehmens.

Risiken der IT-Sicherheit können den Regelbetrieb massiv gefährden. Ein verlässliches IT-System muss alle im Anforderungskatalog definierten Aktionen ausführen, alle nicht definierten Aktionen zurückweisen (z. B. im Hinblick auf datenschutzrechtliche Anforderungen oder solche der Ordnungsmäßigkeit der Rechnungslegung) und das unter den geforderten zeitlichen Rahmenbedingungen. Aus den Zielen der IT-Sicherheit *Vertraulichkeit*, *Integrität* und *Verfügbarkeit* leiten sich weitere Aspekte ab wie *Privacy* (Vertraulichkeit und Integrität einer auf eine natürliche Person zurückzuführenden Information) und *Anonymität* (Vertraulichkeit der Identität einer Person). Auch Eigenschaften wie *Wartbarkeit*, *Flexibilität*, *Stabilität*, *Robustheit* können aufzeigen, wie verlässlich ein System sein kann: Fehlende Stabilität führt schnell zu fehlender Verfügbarkeit und ggf. zu fehlerhaften Daten.

* unter Mitarbeit von Dipl.-Ing., Dipl.-Wirt.-Inf. Dr. Thomas Collenberg

Die Verlässlichkeit eines Systems gewährleistet grundsätzlich aber noch nicht, dass das System/die Anwendung im Sinne der Betroffenen/Anwender funktioniert (ihre Belange berücksichtigt) und für sie nachvollziehbar ist. Um die Nachprüfbarkeit aller Daten, Prozesse oder Ereignisse in einem IT-System sicherzustellen, müssen alle Vorgänge und Ergebnisse (d. h. alle Aktionen und Daten) definierten Auslösern zugeordnet werden können (Authentizität/Zurechenbarkeit/Revisionsfähigkeit). Zurechenbarkeit und Revisionsfähigkeit erfordern, den Blick auf die einzelnen Programmfunktionen eines Systems zu richten. Dies ist insbesondere bei Prüfungen im Hinblick auf die Ordnungsmäßigkeit der Rechnungslegung gemäß Handels- oder Steuergesetzgebung von Bedeutung und ist damit ein typisches Arbeitsgebiet der Internen Revision.

2 Der IT-Security-Prozess

Das Ziel der IT-Sicherheit wird letztlich durch eine unternehmensweit fortlaufend auszuführende Abfolge von Tätigkeiten angestrebt, dem sog. IT-Sicherheitsprozess bzw. IT-Securityprozess. Dieser bezeichnet den von der aus der IT-Strategie abgeleiteten IT-Sicherheits- bzw. IT-Securitystrategie ausgehenden Regelkreis über die Planung, Umsetzung und Überwachung. IT-Sicherheitslücken und die von ihnen ausgehenden Gefährdungspotenziale sind nicht unmittelbar sichtbar und somit in ihren Auswirkungen schwer abschätzbar. Sicherheitslücken entstehen dabei auch durch unkoordinierte oder unvollständige Maßnahmen. Vor diesem Hintergrund ist ein konkreter IT-Sicherheitsprozess, ausgehend von Planung über Umsetzung bis zur kontinuierlichen Überwachung notwendig, um die mit der Anwendung der Informationstechnik verbundenen Risiken zu minimieren. Der IT-Securityprozess beinhaltet ein koordiniertes Vorgehen, um kontinuierlich den IT-Security-Bedarf zu ermitteln (Analyse und Planung), IT-Security-Konzepte zu erstellen (Konzeption), umzusetzen (Realisierung) und regelmäßig zu prüfen, ob die realisierten Sicherheitsmaßnahmen immer noch den aktuellen Anforderungen entsprechen (Aufrechterhaltung, Analyse). Der IT-Sicherheitsprozess ist nicht als konkreter Kernprozess eines Unternehmens zu verstehen. Vielmehr soll er das grundsätzliche unternehmensweite Vorgehen beschreiben, um für alle Prozesse und IT-Systeme geeignete IT-Sicherheitskonzepte zu entwickeln, zielgerichtet umzusetzen und regelmäßig zu überprüfen. Auch diese Überprüfung sollte als typische Revisionsaufgabe angesehen und von ihr wahrgenommen werden. Der IT-Sicherheitsprozess selbst muss alle relevanten IT-gestützten Abläufe im Unternehmen durchdringen.

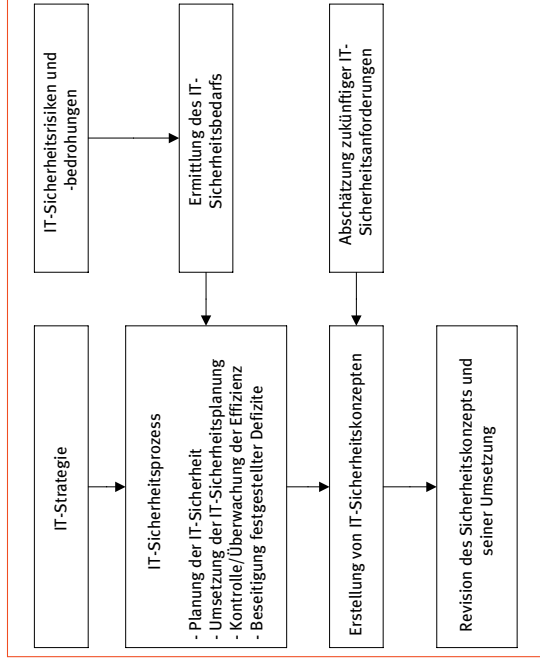


Abb.: IT-Sicherheitsprozess

Der IT-Sicherheits-/IT-Security-Prozess ist nicht nur auf gegenwärtige Anforderungen an die IT-Sicherheit/IT-Security beschränkt, sondern muss vor allem mit ungewissen zukünftigen Anforderungen umgehen können, wobei Security als strategisches Unternehmensziel betrachtet wird. Ob der IT-Sicherheits-/IT-Security-Prozess die im Hinblick auf ungenaue gegenwärtige und ungewisse zukünftige Anforderungen benötigte Effektivität und Effizienz aufweist, ist im Allgemeinen unbestimmt. Die IT-Sicherheits-/IT-Security-Strategie und der IT-Security-Prozess geben strategische bzw. strategisch-operative Ziele insbesondere in der Performance- und in der infrastrukturellen Perspektive vor. Der IT-Security-Prozess kann als Arbeitsobjekt der Revision und des Controllings der IT-Security betrachtet werden. Ein auf die Bedürfnisse des individuellen Unternehmens angepasster und gesteuerter IT-Security-Prozess ist Voraussetzung für die sinnvolle Umsetzung und Erfolgskontrolle von IT-Security-Maßnahmen und somit der Revision der IT-Security, die im Rahmen der Tätigkeiten der Internen Revision vorzunehmen ist. Prüfungsgebiete sind in diesem Zusammenhang Aktivitäten und Ergebnisse, die sich auf den Inhalt und die Umsetzung der IT-Security-Strategie beziehen.

3 Zusammenhang zwischen IT-Security und Geschäftsprozessen

Vor allem wenn Geschäftsmodelle internetbasiert ablaufen, sind sichere IT-Systeme Voraussetzung für den Erfolg der entsprechenden Geschäftsprozesse. Auf die Unterstützung von Geschäftsprozessen auf Basis der umgesetzten IT-Projekte ist das geschäftsprozessbezogene IT-Nutzenpotenzial zurückzuführen. Das IT-Nutzenpotenzial liegt dann darin, die Geschäftsprozesse des Unter-

nehmens effizienter zu gestalten. Über die Unterstützung der Geschäftsprozesse hat sich die IT so zum Business Enabler entwickelt. Die Steuerung des effektiven und effizienten, zweckgerichteten Einsatzes der IT, das Verständnis der strategischen Bedeutung von IT, um so bessere Strategien für die zukünftige Erweiterung des Geschäftsbetriebs zu schaffen, ist Hauptziel der IT-Governance. Die Prüfungsverantwortung sollte hier klar bei der Internen Revision angesiedelt sein.

IT-Governance soll sicherstellen, dass die IT den optimalen Beitrag zur Wertschöpfung des Unternehmens in Bezug auf die Gewährleistung der Unternehmensstrategie und der Unternehmensziele liefert. Produktivitätsbezogene und Business-Value-Vorhaben bieten die Möglichkeit, den wirtschaftlichen Nutzen der IT zu erhöhen. Dabei stehen als Ziele u. a. die Steigerung der Effektivität (die richtigen Dinge tun) und Effizienz (die Dinge richtig tun) der IT im Mittelpunkt. Die Verbesserung von internen Geschäftsprozessen kann z. B. durch die Beseitigung eventuell vorhandener Medienbrüche bei der Übertragung von Daten über Unternehmensgrenzen hinweg erfolgen. Typische Defizite bestehender Prozesslösungen wie zum Beispiel vorhandene Medienbrüche müssen bei einer Prozessrevision festgestellt und im Revisionsbericht offen gelegt werden. Die Verbesserung von internen IT-gestützten Geschäftsprozessen setzt eine hohe IT-Sicherheit (im technisch-organisatorischen Kontext für die IT-Sicherheit von Systemen: Verlässlichkeit und Beherrschbarkeit) der betroffenen IT-Systeme voraus. Insbesondere für Mobile Business Lösungen sind entsprechende Überlegungen sehr erfolgskritisch. Zur Optimierung dieser Nutzenpotenziale sind diese zu maximieren und abzusichern.

Neben technisch-organisatorischen Maßnahmen zur Gewährleistung des störungsfreien Betriebs sind auch Konzepte zum Umgang mit IT-Risiken zwecks Gewährleistung des Regelbetriebs mit größtmöglicher Wertschöpfung bei akzeptablem Risiko von Bedeutung. Grundlage hierfür sollte ein mit der Internen Revision abgestimmtes Risikomanagement-Konzept des Unternehmens sein, welches darüber hinaus die Zielsetzung haben sollte, Ordnungsmäßigkeitsanforderungen auch einschlägiger Gesetze (z. B. KonTraG) zu erfüllen. Entsprechend gehört die Beherrschung von Risiken zu den strategischen Feldern eines Unternehmens; sie sichert den mittel- und langfristigen Geschäftserfolg. Die Forderung an das IT-Management, zunächst den störungsfreien Betrieb sicherzustellen, ist also zu erweitern um die Forderung, Potenziale für eine positive Auswirkung auf den Ertrag/Erfolg des Unternehmens zu schaffen.

Die Absicherung der strategischen Nutzenpotenziale der IT kann durch ein adäquates IT-Security-Management erfolgen, welches im Zentrum der Revision der IT-Security steht. Als IT-Security-Management wird die Planungs- und Lenkungsufgabe bezüglich des IT-Security-Prozesses bezeichnet. Der IT-Security-Prozess ist das Kernstück eines IT-Security-Managements, welches eine angemessene und steuerbare Sicherheit gewährleisten soll. Um bei hoher Dynamik technologischer, organisatorischer und geschäftlicher Veränderungen die erforderliche Sicherheit zu erreichen, ist ein in die Geschäftsabläufe integrierter IT-Security-Management-Prozess unverzichtbar, der seinerseits wiederum gemäß dem PDCA-Zyklus (Plan, Do, Check, Act) sowohl Prüf- als auch Verbesserungsprozesse enthalten muss. Zunächst ist eine IT-Security-Policy zu erstellen, in der das Management einer Organisation die wesentlichen Leitlinien und Regelungen festlegt, die die IT-Sicherheit über den gesamten Verantwortungsbereich gewährleisten soll. In der Phase »Analyse und Planung« sind dann alle relevanten IT-Systeme zu identifizieren und auf Sicherheitslücken zu prüfen. Ferner sind die Risiken bzw. Anforderungen zu bewerten, die durch diese Sicherheitslücken bzw. Kritikalität/Sensitivität entstehen. Auf dieser Grundlage kann dann festgelegt werden, welche Sicherheitslücken bzw. Anforderungslücken zu schließen sind und welche Sicherheitsprojekte aufgelegt werden müssen. In der Phase »Realisierung« sind die Sicherheitsmaßnahmen zu erarbeiten und umzusetzen, um die in der Analysephase festgestellten Sicherheitslücken zu schließen. Das können auch organisatorische Maßnahmen wie Richtlinien, Verfahrens- und Arbeitsanweisungen sein. In modernen ganzheitlich orientierten Sicherheitssystemen werden so auch die konkreten Personen mit ihren Rollen und Aufgaben im Unternehmen geprüft. Die Phase »Aufrechterhaltung« kann in »Check« und »Act« unterteilt werden. Beim Check wird die Einhaltung der Anforderungen überwacht/überprüft und die Wirksamkeit der Maßnahmen durch Neubewertung der verbliebenen Risiken und Erarbeitung von Alternativen zur Risikobehandlung ermittelt. Bei Act werden die Alternativen zur Risikobehandlung umgesetzt sowie interne Richtlinien und Standards angepasst.

4 Geschäftsprozesse und interne Ordnungsmäßigkeitsvorgaben

Aus der Forderung nach der ordnungsgemäßen organisatorischen Abwicklung der Geschäftsprozesse lassen sich interne Ordnungsmäßigkeitsvorgaben ableiten. Wird das Konzept des strategischen Performance-Managements mit Prämissenkontrolle, strategischer Durchführungs-

kontrolle und strategischer Überwachung auf das wie oben definierte Managementsystem übertragen, so müssen die Risiken derart gemanagt werden, dass

- aus den Annahmen abgeleitete Maßnahmen bezüglich der Konformität mit diesen internen Ordnungsmäßigkeitsvorgaben im Hinblick auf IT-Projekte resultierende Anforderungen abgedeckt werden,
- die internen Ordnungsmäßigkeitsvorgaben korrekt umgesetzt werden,
- Fehleinschätzungen, wie kritisch die Konformität mit den internen Ordnungsmäßigkeitsvorgaben bezüglich umzusetzender IT-Projekte ist, aufgedeckt werden.

Bei der Formulierung der internen Ordnungsmäßigkeitsvorgaben orientiert man sich zumeist an bestehenden Standards und Best Practices. Bezüglich der Nutzung von Standards und Normen durch die Interne Revision sei auf verschiedene zu dieser Thematik bereits erschienene Artikel der PRev¹ verwiesen. Bei der IT-Sicherheitsrevision wird die planungsgemäße Umsetzung und Wirksamkeit der Maßnahmen (Standards und Best Practices) überprüft. Dabei wird nicht nur die Einhaltung bestehender Maßnahmen überprüft, sondern auch deren Relevanz im Rahmen der vorgegebenen Ziele. Die ständige und fortlaufende Überprüfung der Relevanz und der Einhaltung bestehender Standards und Best Practices durch die IT-Security-Revision kann auf die Überprüfung der Entwicklung und Umsetzung der IT-Security-Strategie verallgemeinert werden.

Als Konzept zum Umgang mit IT-Risiken zwecks Gewährleistung des Regelbetriebs mit größtmöglicher Wertschöpfung bei akzeptablem Risiko wird das IT-Security-Management daran ausgerichtet. Geeignete Eskalations- und Risikobewältigungsstrategien sowie ein geeignetes Business Continuity Planning (Notfallplanung/Incident Management) zielt auf die Unterstützung/Herstellung der Handlungsbefähigung ab. Durch Etablierung entsprechender Führungskreisläufe, Organisationsstrukturen und Prozesse müssen die Interne Revision und das Controlling zudem erreichen, dass die IT-Strategie und auch die IT-Security-Strategie die übergeordnete Unternehmensstrategie unterstützt. Der IT-Securityprozess ist mit den Unternehmenszielen abzustimmen, da er auf ihnen basiert. Wie bei der Umsetzung der Unternehmensstrategie benötigt das Unternehmen auch bei der Abstimmung der Unternehmensziele mit dem IT-Securityprozess eine entsprechende strategisch-operative Beweglichkeit/Handlungsbefähigung.

5 Controlling und Kontrolle

Im Rahmen des Controllings stehen Struktur und die Eigenschaften von Risiken im Vordergrund. Auch im Rahmen des Managements von Risiken der IT-Security/ des IT-Security-Managements geht es um qualitative (nicht quantifizierbare) Aspekte. Zentrale Fragestellungen des Controllings sind auf die Probleme und die Struktur innerbetrieblicher Koordinations- und Steuerungssysteme ausgerichtet. Controlling gilt generell als geeignet, die Handlungs- und Entscheidungsprozesse im Unternehmen zu koordinieren und zu integrieren. Das Risiko-Controlling hat ein wirkungsvolles Instrumentarium bereitzustellen, um prozessbegleitend das Risikomanagement bei der methodischen Umsetzung zu unterstützen. Auszurichten ist dies an der Aufgabe der zielorientierten Führung der Organisation, welche erfordert, dass das Management Ziele festlegt und das Erreichen dieser Ziele auch durch die Zurverfügungstellung von Ressourcen gewährleistet. Das Controlling kann dementsprechend als managementunterstützende Funktion gesehen werden, die sicherstellen soll, dass die vom Management vorgegebenen Zielsetzungen und Strategien u. a. durch ein adäquates Vorgehen realisiert werden können und so effizient wie möglich erfüllt werden. Dies stellt wiederum eine typische Revisionsaufgabe dar.

Kontrollen im Sinne des Controllings betreffen eher Prognoseunsicherheiten – betrachtet werden vor allem Tendenzen, die zukünftiges Handeln beeinflussen. Die Prüfungen der Internen Revision beziehen sich auf die vom Controlling er- und verarbeiteten Informationen. Gemeinsamkeiten zwischen Interner Revision und Controlling ergeben sich u. a. bei den Indikatoren für die zukünftige Entwicklung: Beide versuchen, die Prognoseunsicherheit aufgrund zunehmender Komplexität und Dynamik der Unternehmensumwelt durch adäquate Instrumente zu begrenzen. So kann sich das Risiko-Controlling an dem Ziel des (sich mit Ungewissheitssituationen befassenden) Risikomanagements orientieren, die Anteile an Ungewissheit zu mindern, indem sie messbar und handhabbar gemacht werden.

Die Ungewissheit der zukünftigen Entwicklungen im Umfeld des Unternehmens erfordert, dass die Aktivitäten zur zielgerichteten Umsetzung von der permanenten Veränderung der ungewissen Umweltbedingungen abhängen. Daher sind durch ein geeignetes Risiko-Controlling entsprechende Entscheidungs-/Handlungsoptionen zu unterstützen. Es geht primär um Konzepte zum

Management und Controlling von strategischen Risiken, d. h. Risiken, die auf der Ungewissheit der zukünftigen Entwicklungen im Umfeld des Unternehmens und daraus resultierender Ungewissheit über die konkreten Zielvorgaben basieren. Ein IT-Security-Controlling kann durch Integration des IT-Security-Managements in ein entsprechendes Risiko-Controlling abgebildet werden.

In diesem Zusammenhang darf das Problem der Restrisiken nicht unbetrachtet bleiben.

Restrisiken sind solche Risiken, die nach klarer Offenlegung und Akzeptanz durch das Management denjenigen Risikobestand bilden, mit denen das Unternehmen »leben« will oder muss.

Restrisiken zeichnen sich dadurch aus, dass ihre Beibehaltung auf zu hohe Kosten stoßen würde, sie nicht zu akzeptablen Bedingungen versicherbar sind oder dass die Wahrscheinlichkeit ihres Auftretens für so gering gehalten wird, dass man glaubt auf ein entsprechendes Risikomanagement verzichten zu können. Die Beobachtung der Entwicklung im Zeitverlauf durch die Interne Revision muss vor allem auch darauf ausgerichtet sein, die Restrisiken einer besonderen Betrachtung zu unterziehen und Erkenntnisse hierüber der Unternehmensleitung unmittelbar und ohne Verzögerungen zugänglich zu machen, um die hierüber gefällte ursprüngliche Entscheidung jederzeit revidieren zu können.



Prof. Dr. Reinhard Vossbein ist Gründungspartner und Geschäftsführer der UIMC Dr. Vossbein GmbH & Co. KG in Wuppertal. Er ist spartenverantwortlich für IT-Management, IT-Sicherheit und toolgestützte Beratung. Außerdem ist er Projektcoach in zahlreichen Beratungsprojekten im Notfallmanagement, im unternehmensorganisatorischen und IV-Sicherheits-Bereich (Banken, Industrieunternehmen, Versicherungen, Sonstige Unternehmen). Weiterhin ist er lizenzierter Lead-Auditor für ISOIEC27001 – auch gem. BSI-Gundschutz.

Dipl.-Ing., Dipl.-Wirt.-Inf. Dr. Thomas Collenberg begann 1980 ein Studium der Elektrotechnik an der Ruhr-Universität Bochum u. a. mit dem Schwerpunkt »Datenverarbeitung«, welches er 1985 als Diplom-Ingenieur abschloss. Danach arbeitete er 11 Jahre lang im Informatik-Bereich, bevor er ab 1997 Wirtschaftsinformatik mit den Schwerpunkten »Betriebliche Kommunikationssysteme« und »Wirtschaftsprüfung« studierte und als Diplom-Wirtschaftsinformatiker abschloss. Anschließend promovierte er an der Universität Duisburg-Essen zum Thema »Revision und Controlling der IT-Security«.

Fazit:

Risiken der IT-Sicherheit können den Regelbetrieb massiv gefährden. Der IT-Security-Prozess kann als Arbeitsobjekt der Revision und des Controllings der IT-Security betrachtet werden. Als IT-Security-Management wird die Planungs- und Lenkungs-aufgabe bezüglich des IT-Security-Prozesses bezeichnet. Der IT-Security-Prozess ist das Kernstück eines IT-Security-Managements, welches eine angemessene und steuerbare Sicherheit gewährleistet soll. Ein IT-Security-Controlling kann durch Integration des IT-Security-Managements in ein entsprechendes Risiko-Controlling abgebildet werden. Die IT-Security-Revision überprüft Effektivität und Effizienz des IT-Security-Controllings.

¹ Vossbein, Reinhard, IT-Sicherheitsnormen als Prüfstandards für die Revision. In: PRev Revisionspraxis, Ausgabe IV/2006, Seite 30–35.