

Risikoorientierte Prüfungsplanung in kleinen Revisionsstäben – Anforderungen an eine Systematisierung

Von Dipl.-Betriebswirt Christoph Wildensee, CISM, Hannover¹

Einführung

Die ‚Risikoorientierte Prüfungsplanung‘ ist bereits seit geraumer Zeit ein wichtiger Teil der Betrachtung revisorischer Leistungserbringung, nicht zuletzt durch gesetzliche Anforderungen an eine Ausgestaltung interner Überwachungssysteme. Entsprechende Vorgaben aus Standards der Wirtschaftsprüfer und nationaler und internationaler Institutionen (ISACA, IIA, IIR) weisen hier konkretisierend den Weg (IDW PS 321/330/340, EPS 523, COBIT etc.).

Insbesondere für Banken bestehen gesetzliche Anforderungen an die Ausgestaltung des Revisionsgeschäftes und ihrer Prüfaktivitäten, die dazu führen, dass sie meist einen umfangreichen Stab an Mitarbeitern aufweisen. Größenordnungen von 30 bis mehr als 50 Revisoren in weltweit operierenden Konzernrevisionen sind durchaus anzutreffen. Entsprechend wird dort (und natürlich auch in anderen Branchen) über umfangreichere Programme sowohl der Einsatz der Revisorinnen und Revisoren als auch die Definition der Prüffelder/Prüflandkarten gesteuert. Es existieren bereits vordefinierte umfangreiche Prüffelddefinitionen, die beliebig erweiterbar, jedoch teilweise stark ‚bankenlastig‘ sind. Dies ist für das Herstellerunternehmen mehr als sinnvoll und macht letztendlich auch das Know-how aus, da sie vollständige/umfassende Leistungen insbesondere im Finanzbereich anbieten kann – somit zählen Banken zu den größten Nutzern.

Für Unternehmen [anderer Branchen], die sich nur wenige Mitarbeiter in der Revision erlauben, ist der Einsatz einer solchen Software schwierig - die vorhandenen Prüffelddefinitionen sind in Detail nur marginal nutzbar, so dass der Einsatz eines solchen Softwarepaketes aus wirtschaftlichen Überlegungen heraus kaum zu rechtfertigen ist. Zudem muss ein solches System auch nachhaltig gepflegt werden. Bei Revisionsstäben mit weniger als 10 Mitarbeiterkapazitäten bedeutet dies einen zu hohen Verlust an Arbeitsleistung und Aufbau von Overhead, insbesondere weil hier die DV-gestützte Mitarbeiterereinsatzplanung nicht zwingend erforderlich ist.

Trotzdem wird auch hier inzwischen erwartet, dass die auf das Unternehmen wirkenden Risiken erkannt, analysiert, revisorisch bewertet und in einen Risiko-Aktivitäten-Kontext gebracht werden. Um hier eine möglichst objektive, nachhaltige und mit einer Historie versehene Beurteilungsmöglichkeit zu schaffen, ist es unausweichlich, die risikoorientierte Planung der Revisionsaktivitäten DV-gestützt erfolgen zu lassen. Der nachfolgende Artikel soll grob die Anforderungen an eine Softwareunterstützung speziell aus Sicht eines kleinen Revisionsbereiches darlegen.

Risiken des Unternehmens

Bevor man sich mit einer detaillierten Beurteilungs- und Analysemöglichkeit auseinandersetzt, ist zu klären, was das Unternehmen als Risiko klassifiziert und ob diese Definition aus Revisions-sicht übernommen werden kann.

Risiken stellen aus Sicht des Unternehmens grundsätzlich eine Aggregation vorhandener, vornehmlich monetär bewertbarer Faktoren dar, die auf die Ertragskraft und Handlungsfähigkeit des Unternehmens wirken - sowohl im Kerngeschäft als auch bei Innovationsprozessen im Sinne der Auswirkung einer ‚Chance‘. Dabei spielt die potentielle Schadenhöhe und die Eintrittswahrscheinlichkeit eine entscheidende Rolle (Einbezug von mathematischen Bewertungsmethoden). Häufig wird nicht das Risiko selbst definiert, sondern auf eine Beschreibung der charakteristischen Risikoeigenschaften und deren Wirkung zurückgegriffen (vgl. KREY, S. 33.).

¹ C. Wildensee ist bei der Stadtwerke Hannover AG als IV-Revisor tätig.

Risiken müssen analysiert, klassifiziert und im Risikomanagement eingebettet sein, so dass sich hieraus Handlungsrahmen/Reaktionspläne (Notfall-/Krisenmanagement u.a.) ableiten lassen. Innerhalb einer solchen Betrachtung liegen auch Risiken im Fokus, die nicht aus dem Unternehmen heraus steuerbar sind, z.B. politische Gegebenheiten, die Mitbewerbersituation, Katastrophenszenarien (z.B. auch Terrorismus u.ä.) oder Umwelteinflüsse.

Die Interne Revision wandelt diese Unternehmenssicht ab. Zum einen klammert sie die aus dem Unternehmen heraus nicht steuerbaren Risiken überwiegend aus, und zum anderen bricht sie Risiken auf die operative Ebene herunter und bildet einen Extrakt, der die Einflussfaktoren beinhaltet, die in der Internen Revision mit überwiegendem Blick auf Zweckmäßigkeit, Organisation, Wirtschaftlichkeit, Ordnungsmäßigkeit und Sicherheit geprüft werden können (vgl. KREY, S. 115ff.).

Dies ist jedoch keine erschöpfende Sicht, vielmehr „kommt es nicht mehr nur darauf an, Risiken zu vermeiden, [...der Fokus liegt] auf der Beurteilung der Effektivität von Management und Kontrolle dieser Risiken. Erst die Kenntnis der Risikopotentiale versetzt die Interne Revision in die Lage, die Funktionsfähigkeit der Überwachungssysteme des Unternehmens zu prüfen. Die Konsequenz ist eine Ausrichtung der Revisionsaktivitäten auf die Risikobereiche des Unternehmens.“ (KREY, S. 20.) Entsprechend integriert die Interne Revision neben der Vermögenssicherung weitere „Zielvorstellungen [wie] das Generieren von Potentialen zur Effizienzsteigerung sowie von Synergieeffekten (u.a. optimaler Ressourceneinsatz) [und] die Überwachung und Sicherung der Zuverlässigkeit von Informationen der Unternehmensführung für das Risikomanagement.“ (KREY, S. 89.) So entsteht eine systematische Zusammenstellung von Prüfungsobjekten, also eine Prüffeldübersicht oder Prüflandkarte, die die im Unternehmen operativ beeinflussbaren Risiken darstellt. Prüffelder sind somit zu verstehen als Zusammenfassung von gleichartigen Risikoeinflussgrößen – (in Kombination) prozess- und funktionsorientiert (vgl. KREY, S. 117ff.).

Prüffeldbezeichnung
[...]
Datensicherung / Recovery / Ausfallsicherheit / Notfallkonzepte IT
Entwicklung von eigenständigen Anwendungen (Programmiersprache, Entwickl.umgeb., CASE etc.)
Installation, Betrieb und Wartung von IT-Komponenten
Kundenabrechnungsprozess
Leistungsverrechnung von IT-(Dienst) Leistungen / IT-Controlling
Manipulation / Missbrauch / Privatnutzung von firmeneigenen IT-Komponenten
Projektmanagement
Organisation und Support bei IT-Prozessen
Risikomanagement (KonTraG)
SAP R/3 – Einsatz/Betrieb und Sicherheit
[...]

Tab. 1: Auszug aus einer Beispiel-Prüffelderliste

Anforderungen an die Beurteilung

„Ein risikoorientierter Prüfungsansatz [...] sollte als Reaktion auf moderne Unternehmensstrukturen die Ausrichtung der Revisionstätigkeit auf die unternehmerischen Risikobereiche und eine daran orientierte Ausgestaltung der Revisionsaktivitäten zum Gegenstand haben. Das erfordert den Übergang von der vergangenheitsorientierten, nur feststellenden [...] zur zukunftsorientierten, innovativen Internen Revision. Dies bedeutet eine Verbesserung der Beratungsfunktion für Management und Fachabteilungen durch zielführende und praktikablere Verbesserungsvorschläge und Anregungen.“ (KREY, S. 21.)

„Die Risikoorientierung führt zu einer Strategie der ‚Prüfung der wesentlichen Risikobereiche‘ des Unternehmens. Risikoorientierung heißt in diesem Kontext:

- Ausrichtung von Prüfungsgegenstand und -umfang an den Fehlerquellen des Unternehmens - Analyse der Unternehmensrisiken

- Ausrichtung an den Fehlermöglichkeiten der Internen Revision - Gestaltung des Prüfungsprozesses zur Gewährleistung der erwarteten Qualität und Sicherstellen der notwendigen Qualifikation der Revisoren.“ (KREY, S. 41.)

Dies darf jedoch nicht dazu führen, dass weniger risikobehaftete Felder keine Beachtung finden. Vielmehr ist für eine Ausgewogenheit zwischen risikoorientiertem Ansatz und einer turnusorientierten Beachtung von Prüffeldern zu sorgen (vgl. KREY, S. 78ff, 203f.).

So ergibt sich bei einer Systematisierung die Notwendigkeit, dass Prüffelder einerseits einer iterativen Risikobetrachtung unterzogen und andererseits mit einem Mindest-Prüfungsabstand definiert werden, der aussagt, innerhalb welches Zeitraumes mindestens eine Prüfung erfolgen muss (Turnusbestimmung). Weiterhin ergänzt die Definition von Mehrjahresprüfplänen den Einbezug des Turnusansatzes, so dass eingesehen werden kann, welche Prüffelder innerhalb eines Zeitraumes bereits geprüft wurden und welche noch ausstehen.

Bewertung von Prüffeldern

Die Bewertung von Prüffeldern gilt als eine besondere Herausforderung, da zum einen Beurteilungskriterien vorhanden sein müssen, die eine [zumindest ansatzweise] objektive Würdigung erlauben und zum anderen durch die Verschiedenartigkeit der Prüffelder eine Ausprägungseinschätzung dieser Kriterien bei der Bewertung oftmals schwierig ist. Als Grundlage für die objektive Beurteilung ist die Definition von Gewichtungsstufen zu sehen, die eine realistische und dauerhafte Abgrenzung der Kriterien untereinander bewirken soll (vgl. KREY, S. 163, 176.).

Weiterhin ist zu klären, welchen Beurteilungsmodus die Interne Revision wählt. Es ist sinnvoll, dass Prüffelder jedes Jahr aufs Neue – jeweils vor Beginn des nächsten Prüfungsjahres – bewertet werden, da sich Risiken durch externe Einflüsse sukzessive verändern (vgl. KREY, S. 164f.), so dass sich jedes Jahr ein komplett neuer Beurteilungslauf für alle Prüffelder ergibt. So ist es möglich, die Entwicklung der Risikoeinschätzung über mehrere Jahre zu beobachten.

Es ist auch denkbar, dass jedes Prüffeld nur initial bei Erstaufnahme bewertet wird und sich die zukünftigen Bewertungen und damit Rangfolgepositionen der Prüffelder ‚maschinell‘ als Fortschreibung aus den Ergebnissen der Prüfungen, die sich auf Prüffelder beziehen, jährlich neu ergeben.

Des Weiteren ist festzulegen, ob bei der Beurteilung bestimmte Prüfkriterien bei ausgesuchten Prüffeldern ausgeblendet werden können oder ob alle Prüffelder mit allen Prüfkriterien bewertet werden müssen (bei Ausblendung besteht die Gefahr des unqualifizierten Vergleiches). Außerdem sollten bei Prüffeldern, aus denen sich jährlich eine Prüfung ergeben muss (z.B. aus einer gesetzlichen Verpflichtung heraus), Bewertungen nicht möglich sein, denn es ergibt sich bereits aus dem Zwang, jährlich zu prüfen, die höchste Rangposition – eine Bewertung und somit Positionsbestimmung ist hier unnötig.

Prüfkriterium
Beachtung im Risikomanagement
Wettbewerbsbedingungen: Abhängigkeit von... Lieferanten/Kunden/Marktveränderungen
Abhängigkeit von der IT
Eindeutige Regelungen/Kompetenzen/Verantwortung/Prozesse...Schnittstellen zu anderen FB...Kontrollen
Ergebnis der letzten Prüfung
Zeitpunkt der letzten Prüfung
Mitarbeiterzufriedenheit / -fluktuation
Kapazitätsauslastung: Auslastung u/o Veränderung der rel. Auslastung im Zeitvergleich
Einhaltung der definierten Bereichsziele
Aufbau- und Ablauforganisation: Änderungen in der Org. in der letzten Zeit u/o Komplexität der Prozesse

Tab. 2: Beispiel-Prüfkriterienliste

Vorausgesetzt, dass die Prüffelder und -kriterien identifiziert sind und die Gewichtung der Kriterien eine sinnvolle Abgrenzung untereinander zulässt, ergeben sich für den Beurteilungsprozess folgende Anforderungen:

Jedes Prüffeld ist mit einer Ausprägung **jedes** Kriteriums zu bewerten. Ausnahme: Wie oben erwähnt dürfen jährlich zu prüfende Prüffelder nicht bewertet werden, da sie aufgrund der jährlichen Prüfnotwendigkeit bereits die höchste Priorität erhalten (müssen). „Die Gefahr eines Risikoeintritts (ausgedrückt durch die Bewertung der Risikofaktoren) und das Ausmaß der Beeinträchtigung der Unternehmensziele (wiedergegeben in der Gewichtung der Risikofaktoren entsprechend deren Bedeutung zur Prozess-/Unternehmenszielerreichung) determinieren damit die Art und Weise des Erreichens der Revisionsziele.“ (KREY, S. 183.)

Weiterhin müssen Prüffelder erweiterbar sein, dabei darf es keinen Verlust an Vergleichbarkeit geben, das Hinzufügen neuer oder Ändern bestehender Prüffelder ist zu historisieren. Gleiches gilt für Prüfkriterien. Prüffeldern sind Mindest-Prüfungsabstände in Jahren zuzuweisen, die definieren, in welchen Abständen die Prüffelder mindestens geprüft werden sollen (Turnusbestimmung). Ihnen sollten auch fachlich zuständige Abteilungen des Unternehmens zugewiesen werden. Die Beurteilung eines Prüffeldes sollte grundsätzlich dauerhaft durch eine Person erfolgen, ein (regelmäßiger/häufiger) Wechsel führt zur Änderung von Wertmaßstäben. Dabei sollten einem Revisor als verantwortlichen Beurteiler ca. 20 Prüffelder zugewiesen werden, da ansonsten diese Art der Risikodarstellung ggf. zu komplex wird (vgl. KREY, S. 169f, S. 176.)

Es ist ein Rollenkonzept und ein gesichertes Login zu implementieren, das die Rollen Administrator, Revisor und Leiter (und ggf. zusätzlich auch Gebietsleiter) beinhaltet. Die Rollenverteilung darf nicht auf eine je Mitarbeiter/-in begrenzt sein. Die Administrationsrolle sollte in der Revision ausgeübt werden. Änderungen an Benutzerstammsätzen wie Hinzufügen, Löschen, Namensänderung oder die Kennwortänderung eines Benutzers durch den Administrator sind zu historisieren.

Während der Beurteilungsphase darf kein Revisor die Rangfolgeposition der ihm zugewiesenen Prüffelder gegenüber denen seiner Kollegen einsehen können, da dies die Beurteilung beeinflusst. Der Beurteilungsprozess für ein neues Planungsjahr sollte bis zu einem bestimmten Datum im alten Jahr, z.B. bis Ende November, abgeschlossen sein. Danach muss die Ermittlung der Rangfolgepositionen der Prüffelder erfolgen, die als „Maß der Prüfungsdringlichkeit interpretiert werden“ (KREY, S. 183.), so dass die Revisionsleitung in der Lage ist, gemeinsam mit jedem/jeder einzelnen Revisor/-in aus der Rangliste heraus das individuelle Prüfprogramm des Folgejahres abzuleiten.

Mit realistischem Blick werden die Prüffelder markiert, aus denen sich eine Prüfung ergibt. Sofern in der Rangfolge hoch angesiedelte Prüffelder keine Prüfung ergeben (z.B. durch fehlende Ressourcen), ist eine Begründung für das Ausbleiben einer Prüfung zu hinterlegen. Prüffelder müssen als Prüfungsvormerkung in der Zukunft markierbar sein. Prüfungsvormerkungen aus der Vergangenheit und Review-Vereinbarungen müssen als Prüfung wählbar sein.

Automatische Prüfungszuweisungen darf es jedoch nicht geben, weil Ressourcenengpässe in kleinen Revisionsstäben Automatismen kaum zulassen. Gleichwohl muss es möglich sein, die Prüffelderrisikosit und die Übersicht der Prüffelder, die außerhalb ihres definierten Prüfungsturnus‘ liegen, gegenüber zu stellen, um beide Darstellungen ausgewogen in die Auswahl der Prüffelder einfließen zu lassen.

Die folgende Tabelle zeigt die Vor- und Nachteile einer solchen Beurteilungsmöglichkeit auf (vgl. KREY, S. 183f.):

Vorteil	Nachteil
Grundsätzlich Förderung systematischer Problembearbeitung	Monetär bewertbare Kriterien verlieren durch Scoring ihre Genauigkeit, können jedoch angemessen berücksichtigt werden
Möglichkeit zur Berücksichtigung verschiedener Zielgrößen mit unterschiedlichen Dimensionen.	Möglichkeit zur Erfassung der Prüfungsziele in Scoringwerten (Dynamik der Unternehmensumwelt)
Fundierte Bestimmung der Risikofaktoren anhand ihres Einflusses auf das Prüfungsrisiko	Erfahrung und Know-how des Revisors bestimmen die Qualität der Prognosen, so werden ggf. „beliebte“ Themen bevorzugt, während bagatellierte/marginalisierte Themen ausgeklammert werden
Flexibilität bei der Zahl der Risikofaktoren je Prüffeld, wobei zum Schutz der Vergleichbarkeit jedes Prüffeld mit jedem Kriterium beurteilt werden sollte	Transparenz der Subjektivität von Entscheidungen
Trotz Komplexitätsreduktion ausreichend große Anzahl von Beurteilungsobjekten und -maßstäben	

Tab. 3: Vor- und Nachteile eines Scoring-Verfahrens mit Bezug zur Nutzwertanalyse

Entsprechend gilt es, ein Scoring-Verfahren zu entwickeln, das mit (ggf. mit der Unternehmensleitung) abgestimmten Beurteilungskriterien und einer angemessenen Abstufung untereinander dauerhaft ein Höchstmaß an Objektivität ermöglicht.

Prüfungsableitung

Nach der Beurteilung der Prüffelder definiert jeder Revisor mit dem Revisionsleiter aus der Beurteilungsmatrix die Prüfungen des Folgejahres als Soll-Vorgabe. So definierte Prüfungen werden im Laufe des Prüfungsjahres mit entsprechenden Echtdateien versehen. Dies können z.B. sein:

- Konkreter Prüfungstitel, Zusammenfassung bzw. Prüfberichtstext, Kenntlichmachung einer Unterstützung durch Externe und Name des Dienstleiters
- Wann wurde die Prüfung eingeplant ?
- Handelt es sich um eine Prüfung aus einer Bewertung heraus oder um ein Review ?
- Wann wurde die Prüfungsvorbereitung begonnen ?
- Wann wurde die Prüfung dem Fachbereich angekündigt ?
- Wann wurde die Prüfung begonnen ?
- Wann wurde dem Fachbereich ein Fragenkatalog übergeben und wann erhielt die IR diesen wieder ausgefüllt zurück ?
- Wann wurde die Prüfung beendet ?
- Seit wann liegt der Prüfbericht vor ?
- Wann fand die letzte Schlussbesprechung mit den beteiligten Fachbereichen statt ?
- Für welches Jahr wurde ein Review aus dem Bericht heraus eingeplant ?
- Wann lag dem Vorstand der Bericht vor bzw. fand die Besprechung beim Vorstand statt ?
- Hinterlegung eines Prüfungsstatus‘ (in Bearbeitung oder beendet)
- Hinterlegung eines kurzen Gesamtergebnisses
- Hinterlegung div. Differenzen zwischen bestimmten Ereignissen, z.B. zwischen ‚Prüfung begonnen‘ und ‚Prüfung beendet‘, ‚Prüfung begonnen‘ und ‚Bericht an Vorstand‘ usw.

Werden vereinbarte Prüfungen nicht durchgeführt, müssen diese als ‚nicht durchgeführt‘ zu erkennen sein und eine Ersatzprüfung ist ggf. zu wählen. Dies muss sich später im Soll-Ist-Vergleich widerspiegeln.

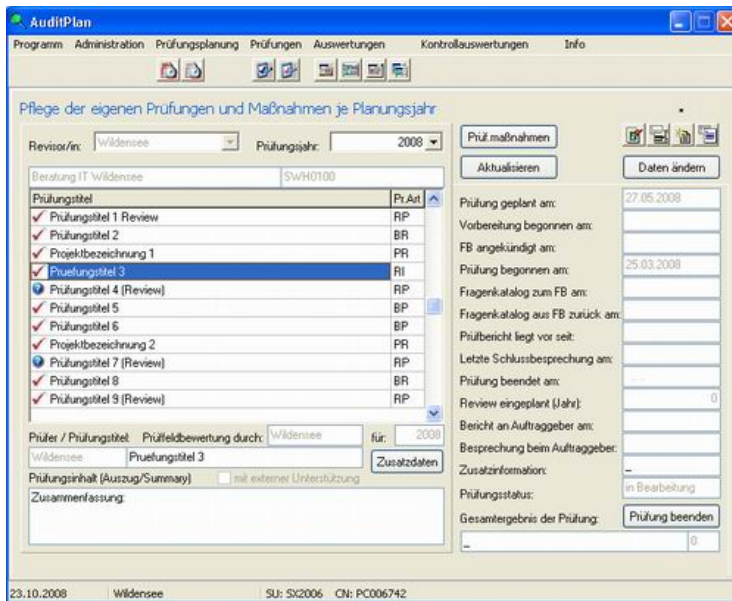


Abb. 1: Beispiel Prüfungsdaten

Beginn und Ende einer Prüfung sind als alleinige Muss-Felder zu definieren, bevor sie beendet werden kann. Es ist möglich, dass eine Prüfung als Beratung endet und sich kein Bericht ergibt, so dass die Berichtsvorlage nicht als zwingend erachtet werden kann.

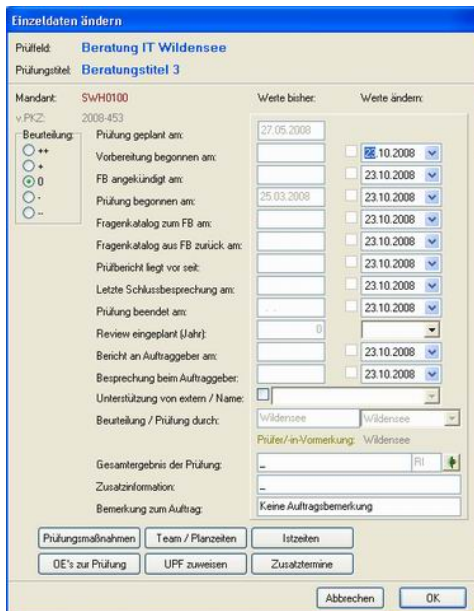


Abb. 2: Beispiel Datenänderung der Prüfungsdaten

Die interne Beratung – auch in Projekten – stellt neben der Prüfung den zweiten, als eigenständige Aufgabe wichtigen Aspekt der Internen Revision dar, der gleichsam ein elementarer Bestandteil des Führungsprozesses des Unternehmens ist (vgl. HUNECKE, S. 51, 64.). „Die Interne Revision kann aufgrund fehlender Anordnungsbefugnis nur eine Unterstützungsfunktion bei der Umsetzung von Verbesserungsvorschlägen übernehmen.“ (HUNECKE, S. 126.) Dies hat sie mit externen Beratungsdienstleistern gemein. Dabei ist es unternehmensabhängig, welche Akzeptanz

Trotzdem ist insbesondere für kleine Revisionsstäbe die Systematisierung der Arbeitsleistung in der beschriebenen Form als Möglichkeit zu sehen, die Entscheidungsfindung des Aktivitäten- / Jahresprüfplanes der Prüfer/-innen zu historisieren und im Nachhinein nachvollziehbar darzustellen. Sie ist ein „fundiertes Auswahlinstrument als ein weniger systematisches einfaches Ranking der bewerteten Risikofaktoren.“ (KREY, S. 183.) Zusätzlich wird nicht nur die gesamte Leistungserbringung der Revision, sondern auch das Optimierungspotential der Unternehmensbereiche und das schlüssige Handeln in Risikobereichen dokumentiert. Durch die Bereitstellung umfassender Auswertungs- und Nachbearbeitungsmöglichkeiten, die flexibel anpassbar sind, stellt die datenbankgestützte Systematisierung eine maßgebliche Dokumentations- und Legitimationsunterstützung revisorischer Leistungserbringung zur Verfügung.

Literatur / Internet-Seiten

- Hunecke, Jörg: Interne Beratung durch die Interne Revision
Diss., Schriftenreihe Rechnungslegung - Steuern - Prüfung,
Band 5, Technische Universität München, 2. Auflage 2003.
- Krey, Sandra: Konzeption und Anwendung eines risikoorientierten Prüfungs-
ansatzes in der Internen Revision, Diss., KPMG, Berlin, 2001.
- Schweiger, Elmar: Beratung durch die Interne Revision - Ihre Rolle,
ihre Risiken und ihre Chancen
In: Zeitschrift Interne Revision (ZIR), 6/2003.
- <http://www.theiia.org/> The Institute of Internal Auditors
- <http://www.isaca.org/> Information Systems Audit and Control Association
- <http://www.idw.de/> Institut der Wirtschaftsprüfer
- <http://www.iir-ev.de/> Deutsches Institut für Interne Revision e.V.
- <http://www.auditplan-xp.de/> AuditPlan ^{XP}