Informationsrisikomanagement: Anforderungen der Finanzaufsicht

Herausforderungen bei der Umsetzung in der Praxis

Als Teil des Risikomanagements müssen sich Factoring- und Leasing-Gesellschaften mit Risiken aus der Informationstechnologie auseinandersetzen. Die bankaufsichtlichen Anforderungen an die Informationstechnologie (BAIT) der Gesellschaften beinhalten spezifische Anforderungen zum Management von drei Risikounterarten des operationellen Risikos. Die konkrete Ausgestaltung des Informationsrisikomanagements ist herausfordernd. Der Autor beschreibt die Systematik eines ganzheitlichen Informationsrisikomanagements und bietet konkrete Lösungsansätze für die Praxis. (Red.)

Spätestens seit der Veröffentlichung der bankaufsichtlichen Anforderungen an die Informationstechnologie (BAIT) im November 2017 ist der Umgang mit Risiken aus der Informationstechnologie ein wesentlicher Bestandteil des Risikomanagements einer jeden Factoring- und Leasing-Gesellschaft. Hierbei ergibt sich die steigende Relevanz für das Management IT-spezifischer Risiken nicht nur aus den regulatorischen Anforderungen, sondern zugleich auch aus einer gestiegenen Bedrohungslage für die IT der Unternehmen sowie einer zunehmenden Digitalisierung von Geschäftsmodellen und -prozessen. Die konkrete Ausgestaltung eines angemessenen und gleichzeitig praktikablen Informationsrisikomanagements stellt die meisten Gesellschaften, wie die Praxis der letzten Jahre gezeigt hat, vor erhebliche Herausforderungen.

SEBASTIAN ADAM

ist Senior Manager bei der Ebner Stolz GmbH & Co. KG Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft, Frankfurt am Main.

E-Mail:
sebastian.adam@ebnerstolz.de

Oftmals beginnt die Schwierigkeit im Rahmen der Umsetzung bereits bei einem einheitlichen Verständnis des Risikobegriffs und setzt sich über die Auswahl eines geeigneten Risikomanagementprozessmodells, der aufbau- und ablauforganisatorischen Ausgestaltung sowie der Integration in das Gesamtrisikomanagement der Gesellschaft fort. Im folgenden Artikel geht es um die Vermittlung eines grundsätzlichen Verständnisses für die Systematik eines ganzheitlichen Informationsrisikomanagementsystems. Zudem werden wesentliche Herausforderungen und Lösungsansätze aus der Praxis aufgezeigt.

Regulatorische Anforderungen an IT-spezifische Risiken

Zur Gewährleistung einer ordnungsgemäßen Geschäftsorganisation müssen Factoring- und Leasing-Gesellschaften nach § 25a Kreditwesengesetz (KWG) beziehungsweise AT 2.2 und AT 4 Mindestanforderungen an das Risikomanagement (MaRisk) über ein angemessenes und wirksames Risikomanagement verfügen. Das Risikomanagement dient insbesondere als Grundlage für eine laufende Beurteilung und Sicherstellung der Risikotragfähigkeit der Gesellschaft. Hierbei sind mindestens die folgenden, aus Sicht der Aufsicht wesentlichen Risiken zu berücksichtigen: Adressenausfallrisiken (einschließlich Länderrisiken), Marktpreisrisiken, Liquiditätsrisiken und operationelle Risiken.

Die BAIT beinhalten in Bezug auf das Risikomanagement der Gesellschaft spezifische Anforderungen zum Management von drei Risikounterarten des operationellen Risikos. Dies sind die Informationsrisiken (IT-Risiken), IT-Projektrisiken sowie Risiken aus dem sonstigen Fremdbezug von IT-Dienstleistungen beziehungsweise (wesentlichen) Auslagerungen. Im Fokus dieses Artikels stehen die Informationsrisiken. Es ist aus unserer Sicht unbedingt anzuraten, eine Betrachtung der anderen beiden Risikounterarten im Rahmen der Ausgestaltung der eigenen Risikotaxonomie der operationellen Risiken vorzunehmen.

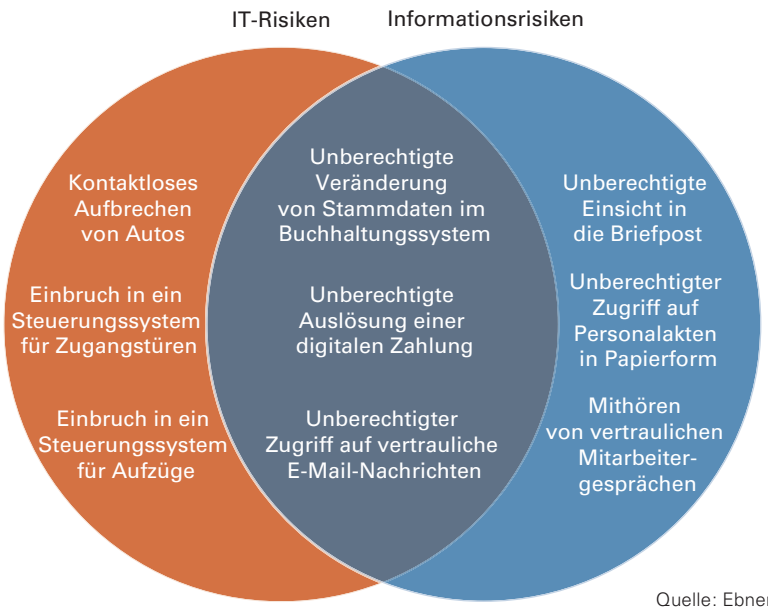
Begriffsverständnis Informationsrisiken

Zum grundlegenden Verständnis der Risikotaxonomie der Gesellschaft in Hinsicht auf das Informationsrisikomanagement ist es wichtig nachzuvollziehen, wie eine Abgrenzung zwischen Informationsrisiken (oder auch Informationssicherheitsrisiken genannt) und IT-Risiken erfolgt. Informationsrisiken und IT-Risiken haben zwar eine große Deckungsmenge, können aber nicht ohne Weiteres einfach gleichgesetzt werden.

So betrachten Informationsrisiken auch Risiken für Nicht-IT-Werte (wie beispielsweise Papierakten), die keine IT-

Risiken darstellen. Zugleich kann es IT-Risiken geben, bei denen der zu schützende Wert keine Information darstellt (wie beispielsweise der Inhalt eines Bargeldautomaten). In der Praxis gibt es hierzu unterschiedliche Ansätze, wobei eine Integration der IT-Risiken in die Risikounterart Informationsrisiko die gängigste Vorgehensweise ist. Dies betrifft ebenso spezifische IT-Risiken, wie beispielsweise die Cyber-Risiken. Das entspricht auch der Denkweise der Aufsicht, die in den vergangenen Jahren den Begriff IT-Risiko nach und nach in ihren Rundschreiben durch das Informationsrisiko ersetzt hat. Wie auch immer die Risikotaxonomie ausgestaltet ist, es muss stets sichergestellt sein, dass alle relevanten Risiken in das Risikomanagement der Gesellschaft miteinbezogen sind.

Abbildung 1: Abgrenzung Informationsrisiko/IT-Risiko



Quelle: Ebner Stolz

Auswahl und Ausgestaltung

Grundsätzlich verfolgen alle Risikomanagementsysteme das Ziel, Risiken zu identifizieren, zu bewerten und zu steuern beziehungsweise zu überwachen. Dies gilt ebenfalls für das Informationsrisikomanagement. Nun gibt es natürlich auch hier unterschiedliche Ansätze für die Ausgestaltung der einzelnen Prozessschritte. Ratsam ist es, sich hierbei an gängigen Standards zu orientieren. Dies ist auch seitens der Aufsicht unbedingt gefordert.

Die zwei bekanntesten Standards für das Umsetzen eines Informationsrisikomanagementsystems sind die ISO-Norm 27005, als verbindende Norm zwischen der ISO 27001 und der ISO 31000, sowie der BSI-Standard 200-3. Beide Standards verfolgen ein ähnliches Herangehensmodell, wobei sie sich im Detail durchaus auch unterscheiden. Die ISO-Norm 27005 ist insgesamt generischer vom Ansatz und bietet daher dem Unternehmen die Möglichkeit einer individuelleren Umsetzung.

Der Ansatz des BSI-Standard 200-3 bietet konkretere Hilfestellungen für die Implementierung, kann aber – wie häufig in der Praxis beobachtet – dazu verleiten, die individuelle Risikosicht der Gesellschaft zu vernachlässigen. Welcher Standard auch herangezogen wird, er sollte auch immer mit den regulatorischen Anforderungen sowie dem Rahmenwerk des Informationssicherheitsmanagements (zum Beispiel der ISO-Norm 27001) im Einklang stehen und diesbezüglich regelmäßig überprüft und gegebenenfalls angepasst werden.

Die erste Herausforderung im Rahmen der Implementierung der einzelnen Prozessschritte des Informationsrisikomanagements betrifft die Identifizierung von Informationsrisiken. Hier gilt es zuerst einmal zu verstehen, über welche Systematik beziehungsweise welchen Kanal Informationsrisiken auf der Grundlage der gängigen Vorgehensmodelle identifiziert werden. Als gängiges Vorgehensmodell ist hier insbesondere der „Anforderungskatalog-Ansatz" zu nennen, der auch in den BAIT im Kapitel zum Informationsrisikomanagement beschrieben wird. Der Ansatz basiert auf einer Erhebung aller Informationskomponenten (Infrastrukturanalyse) und dem daraus erstellten Informationsverbund.

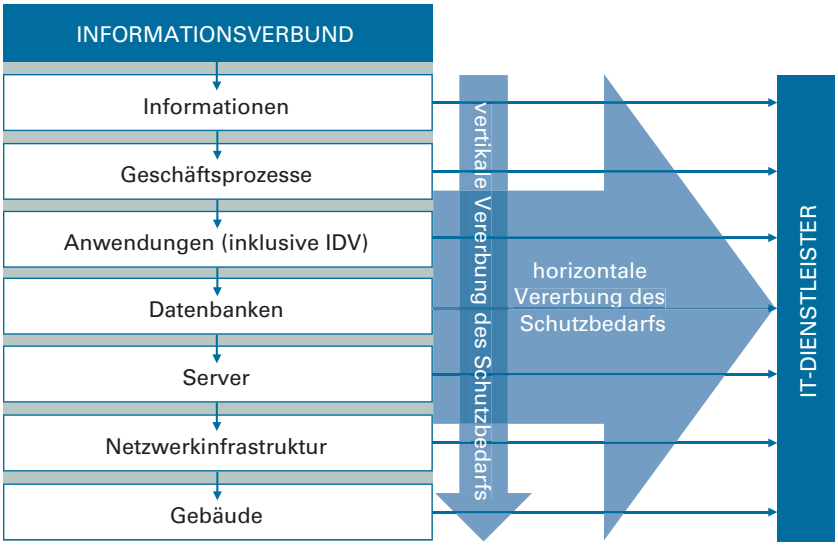
Relevante Informationen

Der Informationsverbund kann hierbei unterschiedlich detailreich ausgestaltet werden. Im Wesentlichen sind hierin jedoch für das Geschäft relevante Informationen als oberste Ebene des Informationsverbundes, Prozesse sowie Teilprozesse – in denen die Informationen als In- und Output-Faktoren verarbeitet werden – sowie für die Prozesse und Teilprozesse relevante Anwendungssysteme, Datenbanken, Server, Netzwerkkomponenten und Gebäude einzubeziehen. Die einzelnen Informationskomponenten sind im Hinblick auf ihre gegenseitige Abhängigkeit bei der Informationsverarbeitung miteinander zu verknüpfen. Diese Verknüpfung der einzelnen Informationskomponenten ist die Grundvoraussetzung für die spätere Vererbung der Schutzbedarfe im Rahmen der Schutzbedarfsfeststellung. Daher ist es auch von so großer Bedeutung, dass die Vollständigkeit der Informationskomponenten (inklusive deren bestehende Abhängigkeiten) sichergestellt ist.

Oftmals besteht in der Praxis die Schwierigkeit, dass keine vollständige Landkarte der Geschäftsprozesse vorliegt, was zu einem erheblichen Aufwand führen kann, wenn diese erst erstellt werden muss. Zugleich zeigt dies bereits beim Aufbau eines Informationsrisikomanagementprozesses, dass das Management von Informations-

risiken eine unternehmensweite und durchaus komplexe Aufgabe ist. Neben den bereits genannten Informationskomponenten ist es dringend ratsam, auch durch die Fachbereiche betriebene oder entwickelte Anwendungen (sogenannte individuelle Datenverarbeitungen) sowie Dienstleister in den Informationsverbund mit aufzunehmen. Durch die Aufnahme von Letzteren in den Informationsverbund wird auch den weiteren Konkretisierungen der Anforderungen der BAIT zum 16. August 2021 nachgekommen, in denen die Vernetzung des Informationsverbundes mit Dritten explizit gefordert ist. Alle Informationskomponenten sind zu inventarisieren und deren Aktualität ist anhand von Kontroll- und Überwachungsmaßnahmen durchgehend sicherzustellen. Als Inventar bietet sich eine Bestandsverwaltung in Form einer Configuration Management Database (CMDB) an.

Abbildung 2: Informationsverbund



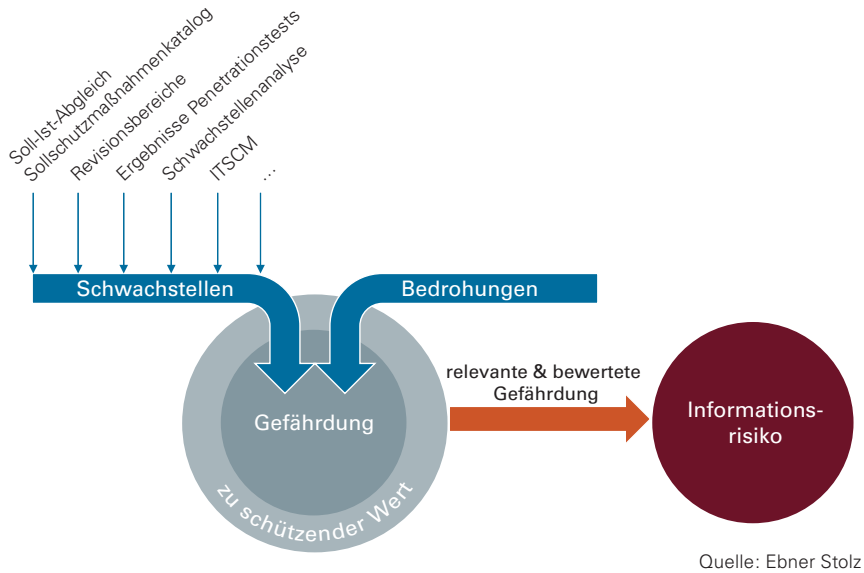
Quelle: Ebner Stolz

Analyse des Schutzbedarfs

Wenn die Grundlage, also ein vollständiger Informationsverbund, geschaffen ist, gilt es, den Schutzbedarf für die einzelnen Informationskomponenten zu bestimmen und mindestens jährlich beziehungsweise anlassbezogen zu aktualisieren. Hierbei sind mindestens die vier Schutzziele Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu bewerten (Hinweis: Die Authentizität wird häufig auch als Teil der Integrität definiert).

Die Schutzbedarfsfeststellung erfolgt in der Praxis häufig noch auf Anwendungsebene. Dies ist nicht zielführend und aus Sicht der Aufsicht auch nicht angemessen, da es bei der Schutzbedarfsfeststellung im Wesentlichen darum geht, das angestrebte Schutzniveau der Informationen zu bestimmen und davon abhängig, das Schutzniveau aller Informationskomponenten, die bei der Verarbeitung der jeweiligen Information eingebunden sind. Zielführender ist, die Schutzbedarfsfeststellungen auf der Geschäftsprozessebene unter Einbezug der hierbei verarbeiteten Informationen durchzuführen. Im Anschluss sind selbstverständlich die ermittelten Schutzbedarfe mit geeigneten Verfahren auf die einzelnen im Geschäftsprozess verwendeten IT-Komponenten zu vererben. Die erfolgten Schutzbedarfsanalysen sowie die hierzu angefertigte Dokumentation ist gemäß den weiteren Konkretisierungen der Anforderungen der BAIT zum 16. August 2021 im Anschluss durch das Informationsrisikomanagement zu überprüfen.

Abbildung 3: Identifikation von Risiken



Quelle: Ebner Stolz

Für die ermittelten Schutzniveaus der Informationskomponenten gilt es, nun Schutzmaßnahmen in Form eines Sollschutzmaßnahmenkataloges zu definieren. Hierbei kann auf bestehende Anforderungskataloge, wie zum Beispiel auf die ISO-Norm 27001 (Annex A) oder auf das IT-Grundschutzkompendium des BSI, zurückgegriffen werden.

Hierbei ist jedoch ausdrücklich darauf hinzuweisen, dass individuelle Anfor-

derungen, die sich beispielsweise aus dem Geschäftsmodell oder der gesellschaftseigenen Gefährdungslage ergeben, mit einbezogen werden sollten. Zudem sind auch spezifische externe Anforderungen wie unter anderem die der Aufsicht (wie die MaRisk, BAIT, EBA GL), die des Bundesministeriums für Finanzen (wie die GoBD) oder die von Gesellschaften, die unter den § 8a BSI-Gesetz (KRITIS) fallen, zu berücksichtigen.

Im nächsten Schritt gilt es nun, auf der Basis der Anforderungskataloge, die beispielsweise aus der ISO 27001 abgeleitet sein können, Schwachstellen zu identifizieren. Hierzu werden Soll-Ist-Abgleiche durchgeführt. Hierbei geht es konkret darum festzustellen, inwiefern die Sollschutzmaßnahmen in Form von Istschutzmaßnahmen in der Gesellschaft umgesetzt wurden. Ein entsprechender Abgleich kann im Rahmen eines risikoorientieren Auditplans oder auch im Rahmen eines den Sollmaßnahmen zu geschlüsselten internen Kontrollsystems erfolgen. Die ermittelten Schwachstellen sind der erste Hinweis auf ein mögliches Risiko.

Bewertung der Risiken

An dieser Stelle stellt sich die Frage, ob ausschließlich über dieses Vorgehen und die hieraus festgestellten Schwachstellen Informationsrisiken identifiziert werden können beziehungsweise sollten. Die Antwort lautet ganz klar nein. Es gibt viele weitere Wege, über die Schwachstellen und damit potenzielle Informationsrisiken zu erkennen sind. Dies sind beispielsweise Ad-hoc-Meldungen aus den Fachabteilungen, Major-Incidents, Feststellungen aus Prüfungsberichten oder Berichten aus Sicherheitsanalysen, wie einem Penetrationstest, festgestellte Abweichungen aus dem Notfallmanagement und der Dienstleisterüberwachung. Daher sollte jede Factoring- und Leasing-Gesellschaft im Zuge des Aufbaus seines eigenen Informationsrisikomanagementsystems individuell für sich eruieren, welche Wege zu betrachten sind.

Mit den identifizierten Schwachstellen geht es nun in den Prozess der Risikoanalyse. Hierbei ist es wichtig zu verstehen, dass Schwachstellen nicht per se eine Gefährdung, beziehungsweise dieser nachgelagert ein Informationsrisiko darstellen. Hierzu müssen noch eine relevante Bedrohung sowie ein Informationswert, der durch die Schwachstelle und die Bedrohung einer Gefährdung unterliegt, hinzukommen. Bedrohungen werden in der Praxis häufig auf Grundlage von standardisierten Bedrohungskatalogen (etwa vom Bundesamt für Sicherheit in der Informationstechnik, BSI) für die Risikoanalyse herangezogen. Um die Bedrohungslage der eigenen Gesellschaft wirklich beurteilen zu können, ist es dringend geboten, regelmäßig auch eigenständig Bedrohungsanalysen durchzuführen, um die spezifische Bedrohungslage der Gesellschaft zu kennen. Dies ist ebenfalls aus Sicht der Aufsicht erforderlich.

Wurden relevante Gefährdungen festgestellt, geht es im Prozessverlauf weiter zur Bewertung des Informationsrisikos (Hinweis: Risiken sind gemäß Definition des BSI relevante und bewertete Gefährdungen). Im Rahmen der Risikobewertung wird der Risikowert (Erwartungswert) anhand des Schadenpotenzials, also der mögliche Schadenswert des Schadensereignisses, sowie der Schadenshäufigkeit, also die Wahrscheinlichkeit des Schadensereignisses, berechnet. Hierzu wird oftmals eine Risikomatrix herangezogen, die zugleich Risikoklassen, unter Einbezug des Risikoappetits der Gesellschaft, beinhaltet. Die Parameter der Risikobewertung innerhalb des Informationsrisikomanagements müssen immer die Werte/Methodik des Risikomanagements der Gesellschaft wiedergeben. Zur Erinnerung: Das Informationsrisikomanagement ist Teil des Gesamtrisikomanagements der Gesellschaft und kann somit nicht anderen Regeln folgen. Die Risikobetrachtung kann hierbei in Form von Brutto- und Netto-Risiken erfolgen. Alle Risiken sind in einem Risikoinventar zu erfassen.

Steuerungsprozesse der Risiken

Die identifizierten und bewerteten Informationsrisiken müssen im nächsten Schritt, wie alle Risiken der Gesellschaft, gesteuert und überwacht werden. Auch hier gilt es, die Methodik und Vorgaben des Risikomanagements der Gesellschaft zu übernehmen. Dies können beispielsweise Regelungen zur Höhe und Genehmigung von Risikoakzeptanzen sein.

Grundsätzlich stehen klassisch folgende Steuerungsoptionen für die Informationsrisiken zur Auswahl: Risikovermeidung (zum Beispiel Workarounds), Risikotransfer (zum Beispiel IT-Versicherungen), Risikominderung (wie zusätzliche Schutzmaßnahmen oder Kontrollen) und Risikoakzeptanz (etwa Akzeptanz von geringeren Risiken durch das Management). Wie die Steuerungsprozesse schlussendlich ausgestaltet werden, ist abhängig vom jeweiligen Risikomanagement der Gesellschaft und kann daher in der Praxis sehr unterschiedlich sein.

Gleiches gilt für die Synchronisierung des vorgelagerten Informationsrisikomanagements mit dem Management der operationellen Risiken. Da Informationsrisiken Bestandteil der operationellen Risiken sind, müssen auch diese im Rahmen der Risikotragfähigkeitsberechnung der Gesellschaft berücksichtigt werden. Hier gibt es in der Praxis unterschiedliche Ansätze wie und ab welcher Höhe die Informationsrisiken hier miteinbezogen werden, sowie in welcher Form die Meldung der Informationsrisiken an das Risikocontrolling erfolgt. Wichtig ist hierbei, dass die Prozesse den Vorgaben des Risikomanagements der Gesellschaft stringent folgen und dass alle Risiken auf der Ebene des Informationsrisikomanagements oder des Risikocontrollings effektiv gesteuert werden.

Damit das Informationsrisikomanagement seinen Aufgaben wirksam und zielführend nachkommt, ist es ebenfalls wichtig, dass eine regelmäßige Evaluierung der Prozesse des Informationsrisikomanagementsystems vorgenommen wird. Das Thema der kontinuierlichen Verbesserung wird derzeit in der Praxis noch stark vernachlässigt. Hier sollten entsprechende interne Kontrollsysteme aufgebaut sowie Management-Reviews in geregelten Abständen erfolgen. Hinweise auf die Effizienz des Informationsrisikomanagementsystems kann hierbei auch die durch die in den BAIT geforderte Berichterstattung an die Geschäftsleitung geben, wenn diese entsprechend detailliert ausgestaltet ist.

Insgesamt ist es empfehlenswert, das gesamte, voran beschriebene Modell zum Informationsrisikomanagement aufgrund der Komplexität über ein integriertes Compliance-Management softwaretechnisch zu steuern.

Herausforderungen für Unternehmen

Abschließend soll an dieser Stelle noch einmal kurz auf die aufbauorganisatorische Ausgestaltung des Informationsrisikomanagements eingegangen werden, da dieses Thema in der Praxis in Teilen Diskussionsbedarfe hervorruft. Das Informationsrisikomanagement ist eine Aufgabe der zweiten Verteidigungslinie des Unternehmens. Somit darf die Funktion nicht durch den Bereich IT, als erste Verteidigungslinie, ausgeübt werden und muss vom Bereich IT unbedingt unabhängig ausgestaltet sein. Für gewöhnlich wird das Informationsrisikomanagement durch das Informationssicherheitsmanagement – oftmals durch den Informationssicherheitsbeauftragten – durchgeführt beziehungsweise von diesem verantwortet. Hintergrund hierfür ist, dass das Informationsrisikomanagement einen der wesentlichen Managementprozesse eines Informationssicherheitsmanagementsystems darstellt (siehe zum Beispiel die ISO-Norm 27001) und somit nur schwierig durch andere Funktionen, wie beispielsweise dem Risikocontrolling der Gesellschaft, verantwortet werden kann. Weiterhin ist für die effektive Steuerung und Überwachung eines Informationsrisikomanagements spezifisches IT-Wissen erforderlich, über das in der Regel nur das Informationssicherheitsmanagement und der Bereich IT in der Gesellschaft verfügt.

Neben der Verantwortung für die Überwachung und Steuerung des Informationsrisikomanagementsystems gibt es noch weitere Aufgaben und Verantwortungen innerhalb der Prozesse des Managements von Informationsrisiken. Dies betrifft insbesondere die Verantwortung für die Bewertung und Steuerung von Einzelrisiken. Diese Verantwortung liegt immer bei dem jeweiligen Risikoeigentümer, der in den meisten Fällen der Eigentümer der durch die Auswirkung des Risikos betroffener Informationen beziehungsweise des Geschäftsprozesses ist. Nur dieser Risikoeigentümer kann eine Entscheidung hinsichtlich Risikobewertung und Risikosteuerung treffen. Das Informationsrisikomanagement kann diese Entscheidung, wie zum Teil in der Praxis gesehen, nicht treffen. Eine beratende Funktion des Informationsrisikomanagements ist hier aber durchaus notwendig.