IT-Governance: Rechtliche Anforderungen an IT-Organisation und Management

Tagung des Schweizer Forum für Kommunikationsrecht (SF-FS), der swiss interactive media and software association (simsa) und des Zentrum für Informations- und Kommunikationsrecht der Universität Zürich (ZIK) vom 28. September 2004

ANNETTE WILLI*

Die enge Verflechtung vieler Unternehmensprozesse mit Informationstechnologie (IT) erfordert eine angemessene Steuerung der Möglichkeiten und Risiken der IT – eine IT-Governance[1]. Dieses aktuelle Thema war Gegenstand einer Tagung des Schweizer Forum für Kommunikationsrecht (SF-FS), der swiss interactive media and software association (simsa) und des Zentrum für Informations- und Kommunikationsrecht der Universität Zürich (ZIK) im Rahmen der Veranstaltungsreihe ICT: Rechtspraxis. Der Tagungsleiter, Dr. Rolf auf der Maur, führte in einleitenden Bemerkungen aus, dass IT-Systeme eine wichtige Voraussetzung für die Funktionsfähigkeit von Unternehmen darstellen. Der Stellenwert der IT-Infrastruktur habe sich von einer Nebenbeschäftigung einiger weniger Freaks hin zur operationellen und strategischen Aufgabe der leitenden Organe einer Gesellschaft entwickelt. Nicht nur die Corporate Governance, sondern auch die IT-Governance müsse deshalb Gegenstand juristischen Interesses und entsprechender Kenntnis sein. In der Schweiz auf rechtlicher Ebene bisher nur wenig diskutiert, sollen die nachfolgend erörterten Referate dazu beitragen, die Anforderungen an die IT-Organisation im Unternehmen und an das Management zu konkretisieren.

I. Elemente und Prozesse der IT-Governance

Der erste Referent, Peter Hill, Infosec South Africa, gab anhand einer Darstellung der charakteristischen Elemente und der Umsetzung der IT-Governance in der Praxis eine Einführung in die komplexe Thematik. Zu Beginn seiner Ausführungen zeigte Hill auf, dass IT-Governance ein wesentliches Element der Corporate Governance darstellt. Er veranschaulichte dies anhand des südafrikanischen Corporate Governance Erlasses (King II), welcher börsenkotierten Unternehmen Vorgaben betreffend ihrer IT-Organisation auf-erlegt. Die IT-Governance sei als Bestandteil der strategischen Ausrichtung des Unternehmens eine Führungsaufgabe, welche, ausgehend von der Initiative des Verwaltungsrates oder der Geschäftsleitung, Top Down umgesetzt werden müsse. Wichtig sei bei der Festlegung einer unternehmensspezifischen IT-Governance die Berücksichtigung der Erwartungen der Stakeholder, die Ausrichtung an der Geschäftstätigkeit und an den strategischen Zielen der Gesellschaft.

Welche Ziele können die Unternehmen mit IT-Governance erreichen? Hill betonte, dass gute IT-Governance nicht nur die Voraussetzungen für die optimale Abwicklung verschiedener Projekte und Prozesse schaffe, sondern vielmehr entscheidend zur Wertschöpfung und schliesslich zu einem Wettbewerbsvorteil des Unternehmens beitrage. IT-Governance ermögliche durch die Ausrichtung der IT an den Erfordernissen des Geschäftes eine Steigerung des Unternehmenswertes, einen verant- wortungsvollen Umgang mit IT-Ressourcen und ein angemessenes Riskmanagement. Um dies zu erreichen, müsse der Umsetzungsprozess klare Zielvorgaben enthalten. Gestützt darauf würden die entsprechenden IT-Aktivitäten gesteuert, kontrolliert und gemessen. Hill betonte, dass vorhandene Organisationsstrukturen eine wichtige Voraussetzung für die Implementierung von IT-Governance darstellten. Von besonderer Bedeutung seien zudem Prozesse als Bestandteile eines IT-Governance Framework; keinesfalls dürfe die Umsetzung von IT-Governance mit der Erstellung eines Dokumentes enden, sondern erfordere die Entwicklung von Prozessen und die Herausbildung entsprechender Fähigkeiten der involvierten Personen. Ein hoher Stellenwert komme dabei der Überwachung und Unterstützung der eingeleiteten Prozesse zu; die Prozessbetrachtung erfolge auf strategischer (doing the

[1] «IT-Governance liegt in der Verantwortung des Vorstands und des Managements und ist ein wesentlicher Bestandteil der Unternehmensführung. IT-Governance besteht aus Führung, Organisationsstrukturen und Prozessen, die sicherstellen, dass die IT die Unternehmensstrategie und -ziele unterstützt.» IT-Governance Institute, IT-Governance für Geschäftsführer und Vorstände, 2. Ausgabe, 11; www. itgi.org.

right things?) und operativer Ebene (doing the things right?). In der Praxis werde zur Umsetzung eines IT-Governance Systems auf Prozessmodelle wie CobiT (Control Objectives for Information and related Technology)[2] und andere Standards[3] zurückgegriffen. Allerdings sollten diese nicht unverändert übernommen werden, sondern an die unterschiedlichen Bedürfnisse der Unternehmen angepasst werden. Ein wesentliches Element der IT-Governance sei schliesslich das Performance Measurement: Es gewährleiste eine Überprüfung der Übereinstimmung von IT-Prozessen mit der strategischen Ausrichtung des Unternehmens und die Messung des Wertbeitrages durch IT. Abschliessend betonte Hill die Wichtigkeit schriftlicher, durch die Unternehmensführung vorgegebener Unternehmensziele für die Entwicklung von IT-Governance-Systemen und die Ausgestaltung der Implementierung als langfristiger Prozess.

II. Auswirkungen des Sarbanes-Oxley Acts und der Eigenkapitalrichtlinie Basel II auf die IT-Governance

Mit den regulatorischen Anforderungen an IT-Governance, insbesondere den Auswirkungen von Sarbanes-Oxley und Basel II auf das IT-Management, befasste sich Dr. Didier Sangiorgio, Rechtsanwalt, Zürich. Als Reaktion auf zahlreiche Finanzskandale in den USA (Enron, Worldcom, Andersen, Xerox) wurde 2002 in der Rekordzeit von 4 Monaten ein neues US-Gesetz (Sarbanes-Oxley Act, SOA) für börsenkotierte Gesellschaften zum Schutze der Anleger erlassen. Sangiorgio nannte sodann als wichtigstes Ziel des SOA auch die Wiederherstellung des Vertrauens in den Kapitalmarkt. Weitgehende gesetzgeberische Interventionen enthalte der SOA v.a. betreffend der Einführung von Audit Commitees, Vorschriften bezüglich der Unabhängigkeit der Revisionsstellen und der Erweiterung der Haftung des obersten Managements. Eine wichtige Hilfsfunktion komme der IT-Governance in Bezug auf die in Section 404 SOA statuierte Verantwortlichkeit des CEO und CFO für die Einführung und Umsetzung eines internen Kontrollsystems zur Überprüfung der in den Geschäftsbericht fliessenden Daten zu. Gemäss Section 302 müssen CEO und CFO eidesstattlich die Richtigkeit und Vollständigkeit sämtlicher Geschäftsabschlüsse beglaubigen und mit ihrer Unterschrift bestätigen, dass sie das interne Kontrollsystem innerhalb der letzten 90 Tage auf dessen Wirksamkeit geprüft haben. Sangiorgio präzisierte, dass CEO und CFO somit persönlich für die Richtigkeit der Erklärung verantwortlich seien und eine Haftungsbefreiung wegen Nicht-Wissens stark erschwert, wenn nicht sogar verunmöglicht werde. Abschreckende Wirkung dürften auch die drastischen Strafandrohungen bei Abgabe einer falschen Bestätigung haben (Busse bis USD 1 Mio. und Zuchthaus bis 10 Jahre bzw. bei Absicht USD 5 Mio. und Zuchthaus bis 20 Jahre). Zur aktuellen Thematik der Auswirkungen des SOA auf die Schweiz führte Sangiorgio aus, dass aufgrund der Anknüpfung am Ort der Börsenkotierung (nicht am Sitz der Gesellschaft) lediglich in den USA zweit-kotierte Schweizer Gesellschaften sowie Schweizer Wirtschaftsprüfer von US-kotierten Gesellschaften in den Anwendungsbereich des SOA fallen. Aufgrund der Ausstrahlungswirkung des SOA sei eine Anpassung von Selbstregulierungsnormen und Best Practice Standards insbesondere auch im Bereich des IT-Managements an Sarbanes-Oxley zu erwarten. Aus den verschärften Dokumentations-, Beweis- und Kontrollpflichten ergeben sich spezifische Auswirkungen auf die IT-Struktur und IT-Prozesse; um diesen Anforderungen zu genügen, sei beispielsweise die Entwicklung eines geeigneten Workflow Management Systems zur Erleichterung der Compliance oder die Einrichtung von Audit Trails zur Gewährleistung der Nachverfolgung der Datenflüsse und Datenveränderungen erforderlich. Eine Erleichterung der Kontrolle und Verringerung des Missbrauchsrisikos sei durch die Schaffung persönlicher Schnittstellen mit Berechtigungsmanagement mittels Benutzerauthentifikation zu erreichen. Ein beachtlicher Dokumentationsaufwand ergebe sich für die Unternehmen aus der Offenlegung, Schulung, Kontrolle sowie Durchsetzung und Revision der erforderlichen Prozesse.

Eine besondere Bedeutung als Rating-Faktor komme der IT-Governance aufgrund der im Juni 2004 durch den Ausschuss der Bankenaufsichtsbehörden der G-10-Länder erlassenen Eigenkapitalrichtlinie Basel II zu. Die Einführung ist in der Schweiz gestützt auf Art. 4 des neuen Bankgesetzes per 31.12.2006 geplant. Basel II soll mittels einer Vereinheitlichung der Eigenkapitalanforderungen an Banken zur Stabilisierung der Bankenstruktur beitragen. Sangiorgio fokussierte im Folgenden auf die operationellen Risiken, die für die Messung der Eigenkapitalunterlegung neben Markt- und Kreditrisi-

[2] Standard für Revision und Kontrolle im IT-Bereich, herausgegeben vom IT-Governance Institute; dazu www.isaca.org/cobit.htm. (2004)

[3] Z.B.: ITIL (Service Management Richtlinie), ISO 17799 (Richtlinie für die Implementierung von IT-Sicherheit), COSO (Vorschläge für ein Kontrollsystem in Unternehmen).

ken in die Beurteilung einzubeziehen sind: Als operationelle Risiken im Bereich der IT seien namentlich Viren- und Wurmattacken, Systemabstürze mit ungenügendem Disaster Recovery, Datenverluste und Verlust der Integrität der Daten oder der Wegfall notwendiger Support- oder Entwicklungsleistungen externer Provider aufzuführen. Die mit diesen Risikoszenarien verbundene Verlustgefahr bilde das operationelle Risiko, welches die Banken bei der Kreditvergabe zu berücksichtigen hätten. Der Einsatz der IT-Governance zur Abwendung operationeller Risiken und zur Steigerung der Ertragskraft durch idealen und strategiekonformen Einsatz der IT-Ressourcen werde somit zum Rating Faktor. Weil die Bank bei hohem Risiko einen höheren Zins vom Kunden verlange, führten Investitionen in die IT-Governance zur Minimierung der Fremdkapitalkosten. Während Basel II auf Seiten der Banken zur Einführung bzw. Weiterentwicklung bestehender CRM-Systeme führe, ergäben sich für die Kunden umfassende Berichterstattungspflichten ge- genüber der Bank. Um der Bank die Beurteilung der IT-Governance zu ermöglichen, sei ein voll integriertes Managementinformationssystem und eine Dokumentation und Kontrolle der Prozesse erforderlich. Nicht zuletzt aufgrund der Bedeutung der IT-Governance für die Minimierung operationeller Risiken sei die Etablierung als eigenständige Disziplin auf oberster Führungsebene zu erwarten.

III. Umsetzung von IT-Governance unter besonderer Berücksichtigung der Verwendung von Standards

Anschliessend sprach Dr. Bruno Wildhaber, CISA, Wildhaber Consulting, Zürich, über Standards und ihren Einsatz bei der Implementierung von IT-Governance. Um IT-Governance wirkungsvoll umzusetzen, müssen Unternehmen in der Lage sein, die Performance von IT-Governance-Initiativen und IT-Prozessen zu messen. Bezugnehmend auf Hill unterstrich Wildhaber das Erfordernis von optimierten Prozessen und Kontrollsystemen zur Performancemessung («You cannot manage what you cannot measure!»). Die Messbarkeit des Entwicklungsgrades von Geschäftsprozessen könne anhand sog. Maturity Levels erfolgen. Dies erlaube eine Beurteilung des aktuellen Standes der Umsetzung von IT-Governance mittels Einteilung in verschiedene Reifestufen. Die Festlegung des Maturity Levels für eine bestimmte Massnahme müsse durch das Management erfolgen und sei an spezifische Unternehmensbedürfnisse bzw. an die Unternehmenssituation anzupassen. Aufgrund der mit Einführung der Methoden wie Balanced Scorecard oder Six Sigma eingeleiteten Entwicklungen gewinne die jederzeitige Messbarkeit und die Nachvollziehbarkeit von Aktionen künftig immer mehr an Bedeutung. Die Tatsache, dass das Management jederzeit in der Lage sein muss, Angaben über die eigene Risk Position zu machen und dies auch messbar darlegen muss, führe weg vom best-Practice-Ansatz hin zu einem führungsorientierten und unternehmensspezifischeren Ansatz.

Für die Implementierung von IT-Governance mittels Tools bestehe in der Praxis ein eigentliches Überangebot an technischen Lösungen; dies allein mache allerdings noch keine IT-Governance aus. Eine wichtige Funktion bei der Umsetzung von IT-Governance komme der Verwendung von Standards zu: Wildhaber führte aus, dass Standards Werkzeuge darstellten, die zur Umsetzung der IT-Governance zur Verfügung stehen. Bei der Verwendung von Standards sei jedoch zu beachten, dass Standards immer ein Abbild ihres Erzeugers darstellten und somit nicht unverändert übernommen werden sollten. Ein sinnvoller Einsatz von Standards sei dann möglich, wenn vorgängig die Ziele und Vorgaben gemäss der IT-Governance gesetzt und die Rahmenbedingungen geklärt seien. Aus der Vielzahl von Standards habe CobiT[4] als Einstiegspunkt für die Implementierung von IT-Governance eine wichtige Bedeutung. Als Audit-Standard entwickelt, umfasse er alle Domänen, die in der IT zum Tragen kommen und beinhalte insbesondere eine Liste von kritischen Erfolgsfaktoren, Elemente zur Performancemessung und eine Darstellung von Maturity Models. Wildhaber betonte allerdings, dass die alleinige Ausrichtung des Unternehmens an Standards nicht ausreiche, um eine Leading Enterprise zu werden. Abschliessend wies der Referent darauf hin, dass die Implementierung von IT-Governance eine klare Eingrenzung der Projekte und die Definition von Meilensteinen und Resultaten erfordere. Gerade wenn externe Berater beigezogen würden, sei wichtig, dass ein Lernprozess initialisiert werde, damit im Unternehmen Fähigkeiten entwickelt würden, welche die Weiterführung des Prozesses gewährleisten.

IV. IT-Governance im Verkehr mit externen Providern

[4] Vgl. Fn. 3.

David Rosenthal, Rechtskonsulent, Zürich, erläuterte Fragestellungen rund um IT-Governance beim Einsatz externer Provider. In jedem Unternehmen spiele die IT-Governance im Beziehungsgeflecht mit aussenstehenden Zulieferern eine wichtige Rolle. Ob bei Dienstleistungen wie dem Support von IT-Systemen oder der Lieferung und Wartung von Software – die Beziehung zu externen Providern wird nach der Erfahrung Rosenthal's oftmals nur ungenügend oder überhaupt nicht geregelt und verwaltet. Anhand verschiedener Beispiele zeigte Rosenthal die häufigsten Defizite im Verkehr mit externen Providern auf: Häufig seien im Bereich von IT-Leistungen keine oder nur mangelhafte Verträge vorhanden. Als Beispiele nannte er den Abschluss eines Gruppenlizenzvertrages ohne Aufzählung der erfassten Gesellschaften oder einen externen Softwareentwicklungsauftrag über CHF 4 Mio. auf der alleinigen Basis einer Grobofferte. Dabei seien Verträge mit dem Provider nicht nur aus rechtlichen Aspekten von Bedeutung, sondern dienten sozusagen als «Lackmustest» zur Klärung der gegenseitigen Erwartungen. Zudem könnten Verträge, neben der wichtigen Verwendungsmöglichkeit zur Dokumentation, als eigenes IT-Governance Tool zur Ordnung und Disziplin beitragen; dies sei zu erreichen, wenn Prinzipien und Vorschriften in den Vertrag aufgenommen würden, die Bestandteil der IT-Governance bilden. Als Beispiele führte Rosenthal Vorschriften über quartalsweise Managementreviews oder die Auferlegung eines Dokumentationzwangs an. Ein weiterer Schwachpunkt liege im mangelnden interdisziplinären Austausch zwischen Juristen, Informatikern und dem «Business». Ein Austausch wäre insbesondere bei der Vereinbarung technischer Spezifikationen und der Festlegung der Vorgehensweise bei Differenzen mit dem Anbieter sowie bei der Festlegung von Service Level Agreements erforderlich. Auch hier seien entsprechende Vorgaben durch das Management zu machen und von den Juristen umzusetzen. Ein weiterer Problembereich liege in der – meist unvermeidbaren – Abhängigkeit des Unternehmens zum Provider; umso mehr drängten sich frühzeitige Überlegungen zur Risikominimierung auf. Als mögliche Lösungs- ansätze nannte Rosenthal beispielsweise ein «Risk-Spreading» über mehrere Partner, die Vereinbarung des Zugangs zum Source Code, die Sicherstellung des Know-how-Transfers oder differenzierte Regelungen zur Vertragsbeendigung. Eine grosse Bedeutung misst Rosenthal der klaren Rollenverteilung im Vertragsverhältnis zwischen Kunde und Anbieter zu. Die Vermeidung von Automatismen und der Gestaltung der Beziehung als Austauschverhältnis statt als Partnerschaft helfe, eine nachlässige Umsetzung der Leistungsvereinbarung zu vermeiden. Die Sicherstellung der Implementierung könne mittels Vorgaben betreffend Umsetzung (in Manuals, Schulungen, Prozessen etc.) und Kontrollmechanismen (mittels Genehmigungs- und Informationspflichten, Audits) gewährleistet werden. Schliesslich sei bei der Vertragsgestaltung darauf hinzuwirken, dass zentrale Fragen nicht offen bleiben, sondern geklärt und festgehalten werden; gerade im internationalen Geschäftsverkehr sei das Risiko einer unterschiedlichen Auffassung aufgrund unterschiedlicher Kulturen sehr hoch. Rosenthal warnte jedoch vor einer starren Ausgestaltung der Verträge. Die ständige Weiterentwicklung der Informatik erfordere vielmehr den Einbau von Änderungsmöglichkeiten und Reviews; blosse Change Requests genügten nicht. Zum Schluss ermutigte Rosenthal nochmals zur Verwendung von Verträgen als IT-Governance-Instrumente und gab zu bedenken, dass bei der Auslagerung von Informatik-Leistungen die Verantwortlichkeit dafür grösstenteils beim Kunden verbleibe.

V. Rechtliche Verantwortung für IT-Governance

Zum Abschluss referierte Peter Höltschi, Zürcher Kantonalbank, über die rechtliche Verantwortung des Managements und Verwaltungsrates für IT-Governance. In Ergänzung zum Referat von Sangiorgio legte Höltschi den Schwerpunkt auf Vorschriften des Schweizer Gesellschaftsrechts, Softlaw und Aufsichtsrechts für Banken. Anknüpfungspunkt für die Ableitung einer Verantwortlichkeit des Verwaltungsrates bildeten die Bestimmungen des Aktienrechts bezüglich Oberleitung und Oberaufsicht des VR im Rahmen der unübertragbaren Aufgaben (Art. 716a OR) und die im Swiss Code of Best Practice für Corporate Governance (SCBP) enthaltenen Pflichten, insbesondere Ziff. 13 bereffend der Pflicht, für ein Kontrollsystem und ein Risikomanagement zu sorgen und Ziff. 20 bezüglich der Massnahmen zu Einhaltung der anwendbaren Normen (Compliance). Spezifische Bestimmungen für Banken ergeben sich aus dem Bankengesetz (Art. 3 Abs. 2 lit. a BankG), den Richtlinien zur internen Kontrolle und dem Rundschreiben der Eidgenössischen Bankenkommission (EBK-RS 96/3) betreffend des Revisionsberichts. Zusammenfassend hielt Höltschi fest, dass von den genannten Bestimmungen nur das Aufsichtsrecht der Banken eine über

die allgemeinen Governance-Normen hinausgehende Verpflichtung betreffend IT-Organisation enthält. Am Beispiel einer Bank führte Höltschi aus, dass die IT unabdingbar sei für die Strategieerreichung, sowie als unterstützendes Element der internen Kontrolle, des Riskmanagements und der

Compliance ein wichtiges Kontrollmittel darstelle; durch die Beanspruchung von ca. 20–25 % der Betriebskosten sei die IT allerdings auch als einer der grössten Kostenfaktoren zu qualifizieren. Höltschi kam zum Schluss, dass sich der Verwaltungsrat aufgrund dieser zentralen Stellung der IT zumindest auf einer strategischen Ebene mit IT befassen müsse; so etwa bei der Festlegung der Geschäftsstrategie und deren Auswirkungen auf die langfristigen unternehmerischen Handlungsoptionen, beim Einsatz der Finanzmittel und im Rahmen seiner Verantwortung für die Umsetzung von Kontrollmechanismen. In Abgrenzung dazu sei die Geschäftsführung auf einer taktischen Ebene für organisatorische und technische Vorgaben und Vorschriften bezüglich IT und auf einer operativen Ebene für die Umsetzung zuständig. Als Beispiel erwähnte Höltschi das IT-Lizenzmanagement und das IT-Vertragsmanagement als Managementaufgabe auf der taktischen Ebene. Beim Lizenzmanagement erschwerten unterschiedliche Lizenzmodelle der Anbieter von Betriebssystemen oder Applikationssoftware die Umsetzung einer Unternehmensstrategie. Konkret sei deshalb eine proaktive Steuerung des Lizenzmanagements durch Festlegung von Grundsätzen beim IT-Einkauf sowie deren Umsetzung und Kontrolle angezeigt, beispielsweise durch Vorgaben betreffend Lizenzparameter, Nutzungsrechte im Konzern, Mandanten- oder Outsourcingrechte. Höltschi wies allerdings auch auf die Durchsetzungsproblematik von IT-Governance-Prinzipien des Nachfragers gegenüber dem externen Anbieter von IT-Dienstleistungen hin. Der Gestaltung des Vertragsmanagements komme insbesondere unter Basel II ein hoher Stellenwert zur Vermeidung von Rechtsrisiken zu. Als Aussage mit gewisser Signalwirkung für die Frage der Verantwortung des VR für IT-Governance ist die abschliessende Bemerkung Höltschi's zu werten, wonach die ZKB die Einführung eines IT-Verwaltungsratsausschusses vorbereite.

VI. Spezifische IT-Kenntnisse als Anforderung an den Verwaltungsrat?

Die anschliessende Diskussion war geprägt von der Problematik rund um die Verantwortlichkeit des VR für IT-Governance. Im Zentrum stand die Frage, ob der VR spezifische Kenntnisse im IT-Bereich haben müsse. Während verschiedene Referenten eine entsprechende Kompetenz mindestens eines VR-Mitglieds forderten, vertrat Rosenthal die Ansicht, dass es nicht unbedingt einen IT-kundigen Verwaltungsrat brauche und wies auf die Bedeutung der Revisoren für die IT-Governance hin. Der Verwaltungsrat müsse aufgrund von Berichten entscheiden, auf welchem Maturity Level sich die Gesellschaft befinde und gestützt darauf gegebenenfalls die notwendigen Prozesse einleiten. Nach seiner Erfahrung stelle der VR einen Handlungsbedarf oft erst dann fest, wenn die Revisionsberichte darauf aufmerksam machten; der Grund hierfür liege in Kommunikationsproblemen zwischen den IT-Verantwortlichen und den leitenden Organen einer Gesellschaft. Demgegenüber wies Wildhaber auf die Gefahr hin, die Revisionsstellen als Meldungssysteme für IT-Probleme bzw. als Garant für korrekte IT zu sehen; explizite IT-Revisionen würden meist nur bei den grossen Gesellschaften durchgeführt; bei kleineren Gesellschaften bestehe dafür kein Budget. Seitens der Zuhörerschaft wurde eine eher zurückhaltende Meinung bezüglich persönlicher IT-Kenntnisse des VR vertreten und als Lösungsansatz die Bildung interner IT-Audits mit direktem und unabhängigem Mandat vom VR oder der Beizug externer Fachpersonen vorgeschlagen. Übereinstimmend wurde von mehreren Referenten festgestellt, dass Probleme mit IT-Projekten oftmals nicht auf mangelndem technischem Verständnis des VR oder falscher Beurteilung der technischen Möglichkeiten von IT beruhen, sondern vielmehr das Geschäft oder der Markt falsch eingeschätzt werde. Vielen Problemen lägen auch die mangelnde Begleitung und Überwachung des Projektverlaufes durch den VR zugrunde. Spielten solche betriebswirtschaftlichen Probleme eine Rolle, habe der Verwaltungsrat dafür geradezustehen.

Die Tatsache, dass in der Schweiz bisher noch keine Gerichtsentscheide zur Verantwortlichkeit für IT-Governance ergangen sind, darf nicht darüber hinwegtäuschen, dass der erwartete Bedeutungszuwachs der IT auch rechtliche Konsequenzen mit sich bringen kann. Eine Klärung der Verantwortlichkeiten und Zuständigkeiten für IT-Governance ist angebracht, um der IT-Governance als integraler Bestandteil der Unternehmensstrategie und Unternehmensführung gerecht zu werden.

* lic. iur., wissenschaftliche Assistentin am Rechtswissenschaftlichen Institut der Universität Zürich.