Hintergrund-Interview zu IT-Risk-Management und -Compliance

Nutzen aus gesetzlichen Regeln ziehen

IT soll die Unternehmensstrategie und -ziele unterstützen. Dazu gehört „IT-Compliance" – das sich halten an gesetzliche und vertragliche Regelungen. Doch gerade stetig neue gesetzliche Regelungen bringen IT-Abteilungen in Schwierigkeiten. *geldinstitute* befragte Joachim Hörnle, Geschäftsführer von Blue Elephant Systems, wie sich IT-Compliance mit IT-Risk-Management unter einen Hut bringen lässt.

Wieso sind die Anforderungen an IT-Governance gerade im Finanzsektor besonders hoch?

Joachim Hörnle: Die letzte Finanzkrise hat die Regulierungsbehörden sensibilisiert und darin bestärkt, den Banken schärfere Regeln zur Überwachung und Kontrolle aufzuerlegen. Zu nennen sind unter anderem das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) für ein rechtssicheres IT-Risikomanagement, Supervisory Review and Evaluation Process (SREP) gemäß der Säule II der Basel-II-Umsetzung und die Berücksichtigung von Counterparty Credit Risks (CCR) gemäß Basel II. Hinzu kommen der § 25a des Kreditwesengesetzes. Er schreibt den Kreditinstituten eine angemessene technisch-organisatorische Ausstattung sowie ein angemessenes Notfallkonzept für IT-Systeme ins Pflichtenheft. Die MaRisk-Module AT 7.2 und 7.3 der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) konkretisieren die Anforderungen ans interne Steuerungs- und Kontrollsystem für ein modernes IT-Risikomanagement. Die MaRisk-Module verweisen dazu auf den IT-Grundschutzkatalog des Bundesamts für Sicherheit in der Informationstechnik (BSI) und auf den internationalen Sicherheitsstandard ISO/IEC 2700X.

Wie lange wird es dauern, bis der Finanzsektor die Auswirkungen spührt?

Joachim Hörnle: Die Entwicklung läuft erst an. Es werden also weitere Regularien für die Geldhäuser hinzukommen. Hinzu kommt der interne Druck in den Finanzinstituten, im eigenen Interesse mehr für die Transparenz und Kontrolle ihrer Geschäftsabläufe zu tun. Weil die Geschäftsabläufe zunehmend IT-gestützt ablaufen, ist es mehr als konsequent, den Risikomanagement- und Compliance-Hebel genau hier, innerhalb der IT-Infrastruktur, anzusetzen. Für ein professionelleres IT-Governance in den Finanzinstituten spricht nicht nur der sich erhöhende Regulierungsdruck von innen und außen. Auch aus kaufmännischer Sicht ist es ratsam, IT-Risikomanagement und IT-Compliance stärker zu fokussieren und konsequent

Joachim Hörnle, Geschäftsführer von Blue Elephant Systems.

umzusetzen. Dazu müssen die Unternehmen von Grund auf mehr Effizienz, Transparenz und Kontrolle in ihren IT-Betrieb bringen.

Wieso ist diese höhere Effizienz, Transparenz und Kontrolle im IT-Betrieb für Banken so wichtig?

Joachim Hörnle: Sie bilden die Basis für IT-Governance, also für ein besseres Risikomanagement und mehr Compliance. Nur wenn

- → der IT-Betrieb optimiert wird,
- → Prozesse darin transparent gestaltet werden,
- → Kontrollen im IT-Betrieb harmonisiert und weitgehend automatisiert werden, und
- → Prozesse zur Erfassung, Aufbereitung, Verarbeitung und Analyse relevanten Infomationen selbsttätig ablaufen,

ist das hohe Ziel überhaupt erreichbar: ein profundes IT-Risikomanagement und mehr IT-Compliance, und dies zu insgesamt budgetvertretbaren Kosten. Den IT-Betrieb zu optimieren, das funktioniert aber nur, wenn es dem Finanzinstitut gelingt, das technische und geschäftsorientierte IT-Management unter einen Hut zu bringen.

Wieso heben Sie diese Integration von technischem und geschäftsorientiertem IT-Management heraus?

Joachim Hörnle: Ohne diese Integration, leider heute in den meisten Finanzinstituten der Status quo, sind die Unternehmen mit vielen negativen Folgen konfrontiert: hohe IT-Betriebskosten, geringe IT-Leistungserbringung und vor allem hohe betriebliche Risiken.
Zudem bleiben ohne die notwendige Transparenz und Kontrolle im IT-Betrieb für die Verantwortlichen die tatsächlichen Kosten, Leistungen und Risiken weitgehend im Dunkeln. Die Folgen: Weder die Kostentreiber noch die Risiken können enttarnt werden. Das gilt sowohl für den IT-Betrieb als auch für die Auswirkungen der betrieblichen Störungen auf geschäftlicher Ebene.

Somit können die Verantwortlichen, was den IT-Betrieb und darauf aufsetzend die geschäftlichen Abläufe betrifft, mehr oder weniger nur aus dem Bauch entscheiden. Dies alles unterhöhlt natürlich die Qualität von IT-Governance. Dies, obwohl die Entscheider gerade im Finanzsektor verstärkt in der Pflicht stehen, dass sowohl IT-Risikomanagement als auch IT-Compliance im Unternehmen verlässlich und nachweislich greifen müssen.

„Es ist wichtig, dass die geschäftlichen und IT-Entscheider an einem Strang ziehen. Die Hauptaufmerksamkeit der Überwachung, Kontrolle und Steuerung sollte dennoch den IT-Komponenten innerhalb der IT-Infrastruktur gelten." Joachim Hörnle

Blue Elephant Systems

Wie sollte das IT-Management als Grundlage für IT-Governance im Institut ganzheitlich aufgesetzt werden?

Joachim Hörnle: Es ist wichtig, dass die geschäftlichen und IT-Entscheider an einem Strang ziehen. Die Hauptaufmerksamkeit der Überwachung, Kontrolle und Steuerung sollte dennoch den IT-Komponenten – Anwendungen, Server und Netzwerksystemen – innerhalb der IT-Infrastruktur gelten. Im Fokus der Betrachtung sollten die IT-Komponenten stehen, die für die laufenden Geschäfte einen tragenden Charakter haben und deren Ausfall oder unzureichendes Funktionieren für das Institut hohe Risiken und hohe Kosten in sich bergen. Diese Risiken und Kosten gilt es sowohl von der Warte des IT-Betriebs als auch des Geschäfts zu analysieren und zu bewerten. Nur dadurch wird der volle Umfang der Risiken und Kosten transparent. Und nur so können im Einzelnen die Aufwendungen für das IT-Risikomanagement und für IT-Compliance einerseits und der Nutzen dieser Maßnahmen – Kosteneinsparungen, Risikominimierung und mehr Regelkonformität – andererseits konkret abgeschätzt werden.

Erst danach steht die Auswahl geeigneter IT-Management-Werkzeuge an, um darüber von Grund auf IT-Risikomanagement und IT-Compliance mit Augenmaß umzusetzen. Natürlich müssen darüber hinaus, das konkrete Anforderungsprofil vor Augen, die künftigen Überwachungs-, Verarbeitungs- und Informationsroutinen herausgearbeitet werden.

Wir bieten dafür zum Beispiel die MIDAS-Produkt-Suite an.

Und wie findet man das richtige Anforderungprofil?

Joachim Hörnle: Für eine angemessene Überwachung, Kontrolle und Steuerung der geschäftstragenden IT-Komponenten und für eine gezielte, werthaltige Informationsgabe für IT-Risikomanagement und IT-Compliance müssen die Entscheider folgende Fragen beantworten:

- → Wie und in welchen Zeitintervallen sollten und müssen die kritischen IT-Komponenten überwacht werden?
- → Wie sollten die Schnittstellen zwischen der Überwachungskonsole und den zu überwachenden IT-Komponenten realisiert werden?
- → Wie sollten Störungsmeldungen ermittelt werden, um bei Ausfällen oder Einschränkungen in IT-Komponenten zu aussagekräftigen Informationen zu gelangen?
- → Welche Ausnahmesituationen müssen behandelt werden?
- → Welche Störungen innerhalb der IT-Komponenten müssen dazu erkannt werden?
- → Wie sind Informationen über Störungen weiterzuverarbeiten?
- → Welche korrigierenden Aktionen müssen bereitstehen, die im Störungsfall automatisch die Ausführung übernehmen können?
- → Wer ist im Störungsfall zu benachrichtigen?
- → Welche technischen Mittel müssen bereitstehen, um eingehende Störungen gezielt und schnell bearbeiten zu können?
- → Und, ganz wichtig: Welche Prozesse zur Erfassung, Aufbereitung, Verarbeitung und Analyse von IT-Governance-relevanten Informationen sollten automatisiert ablaufen, um ein qualitativ hochwertiges und kostensparendes IT-Risikomanagement umsetzen und Regularien und Regeln lückenlos befolgen zu können?

Die Qualität des IT-Risiko-Managements und der -Compliance fällt doch mit der Qualität der für IT-Governance wichtigen Informationen und dem Automatisierungsgrad der Informationsprozesse?

Joachim Hörnle: So ist es. Die Qualität der Informationsbasis, die den künftigen Kontroll- und Steuerungssystemen für IT-Risikomanagement und IT-Compliance zugrunde liegt, muss ausgesprochen hoch sein. Die sachliche Richtigkeit und Aktualität dieser Informationen ist dafür unumgänglich. Sie kann nur über eine permanente und enge Zusammenarbeit von IT und Business erreicht werden. Die technische Herausforderung besteht darin, die Menge der zu verarbeitenden Informationen, ihre unterschiedlichen Datenformate und -quellen sowie ihre häufigen Änderungen wirtschaftlich zu bewältigen. Die Automatisierung der Erfassung, Aufbereitung, Verarbeitung und Analyse der Informationen trägt dazu bei, dass manuelle, fehlerträchtige Brüche vermieden werden, die sich ansonsten negativ auf die Qualität des IT-Risikomanagements und von IT-Compliance auswirken würden. Zudem können per Prozessautomatisierung Routineaufgaben im Rahmen von IT-Governance vereinfacht und beschleunigt werden. Nur wenn diese Voraussetzungen erfüllt sind, werden die Verantwortlichen in den Finanzinstituten auf ein hieb- und stichfestes IT-Governance bauen und dafür jederzeit angemessene Entscheidungen treffen können. Für die Herausbildung einer leistungsfähigen und wirtschaftlichen IT-GRC-Lösung sollten die Entscheider innerhalb des Werkzeug-Sets wie MIDAS von Blue Elephant Systems besonders auf den Einsatz erprobter und standardisierter Verfahren, die Wiederverwendung bestehender Daten und Werkzeuge sowie einen hohen Automatisierungsgrad der Beschaffung und Aufbereitung von IT-Governance-Informationen achten. ■

Das Interview führte Hadi Stiel, freier Journalist in Bad Camberg.