Umfassende Risikobetrachtung durch Business- und IT-Audit

Von Olga Valek und Peter Marti

Eine umfassende Risikobetrachtung der ganzen Unternehmung kann gefördert werden durch verbesserte Zusammenarbeit und Kommunikation zwischen Business- und IT-Audit. Im Januar 2017 findet eine gemeinsame Konferenz von SVIR und ISACA statt.

Artikel erschienen in Swiss IT Magazine 2016/12

In den letzten Jahren hat sich die Informatik in den meisten Firmen und Branchen von einer technischen Backoffice-Dienstleistung zu einem treibenden und kritischen Träger der Business Prozesse entwickelt. Die Verzahnung zwischen den Businessprozessen und der Informatik hat sich so stark intensiviert, dass jedes technische Husten in der Informatik sich oft unmittelbar mit Schüttelanfällen im Business bemerkbar macht. Ein Stillstand der Informatik könnte gar Krisen auslösen und das Überleben der Unternehmung in Frage stellen. Daher ist es konsequent und nachvollziehbar, dass Risikobetrachtungen vermehrt unternehmensweit erfolgen und neben den wertschöpfenden Business-Prozessen auch die unterstützenden Prozesse und Systeme der Informatik adäquat mitberücksichtigt werden.

In grösseren Organisationen wird das unternehmensinterne Audit häufig in zwei dedizierten Units aufgebaut: als Business- wie auch als IT-Audit. Beide Teams haben einen entsprechenden Fokus und Expertise, aber auch ihre Grenzen. Das IT-Audit versteht sich zwar in den technischen Prozessen und Systemen souverän zu bewegen. Das Business-Audit hat seinerseits eine hohe Kompetenz der Geschäftsabläufe und Wertschöpfungskette. Aber Beiden ist die Expertise des anderen Teams verwehrt. Darum ist es umso wichtiger, dass die beiden Einheiten einen aktiven Informations-austausch leben, sich über den eigenen Gartenzaun hinauslehnen und sensibilisiert sind für Wechselwirkung zwischen den IT und Business Prozessen:

• Welche Business-Prozesse werden mit welchen IT-Applikationen umgesetzt?
• In welchen IT-Systemen sind hochsensible Geschäftsinformationen gespeichert?
• Wie sind die Abhängigkeiten wischen IT- und Business-Controls?
• Wie sieht die Beziehung einer Business-Rolle zu den darunter liegenden Applikations-User aus?

Integrated Audit

Unter dem Begriff "Integrated Audit" werden verschiedene Formen der Zusammenarbeit dieser beiden Audit-Units diskutiert und wie die unterschiedlichen Risk-Frameworks miteinander in Bezug gesetzt werden können (zB Mapping zwischen dem COSO-Würfel und dem COBIT-Modell). Letztendlich bleibt aber die Wichtigkeit einer aktiv gelebten Kommunikation zwischen IT-Audit und Business-Audit. Damit wird die Sensibilisierung zum anderen Audit-Team gestärkt. Konkrete Informationen zur vertieften Analyse können bei Bedarf weiter gereicht oder bei gemeinsam geplanten Audits die Risikobeurteilung wesentlich erhöht werden.

Auditverbände in der Schweiz

In der Schweiz werden Business- und IT-Audit von zwei unterschiedlichen Verbänden gefördert und unterstützt: SVIR (Schweizerischer Verband für Revision) und ISACA (Information Systems Audit and Control Association). Diese beiden Verbände sorgen gemäss ihrem Kernauftrag dafür, dass das Business- wie auch IT-Audit in der Schweiz thematisiert, optimal gestärkt und aktiv mit Schulungen gefördert wird.

SVIR - ISACA Konferenz

Nach einer Ruhepause von fast zwei Jahren laden SVIR und ISACA wieder zu einer gemeinsamen Konferenz in Zürich ein.

IIA in der Schweiz

Cyber Risks stellen nicht nur ein Schlagwort der aktuellen Zeit dar, sondern gehören in der Kategorie der technologischen Risiken gemäss dem WEF-Report 2016 zu den grössten globalen Risiken. Als Schweizer Vertretung (Schweizerischer Verband für Interne Revision – SVIR resp. IIA Switzerland) des internationalen Dachverbandes Institute of Internal Auditors (IIA) mit Sitz in Florida, USA sind wir generell daran interessiert, dass alle Unternehmen resp. Organisationen, privat sowie öffentlich, in der Schweiz und in Liechtenstein alle Arten von Risiken ganzheitlich überwachen und ein wirksames Risk Management aufweisen, welches regelmässig vom Internal Audit überprüft wird. Die Gründung des IIA geht auf das Jahr 1941 zurück und zählt etwa 190’000 Mitglieder aus 170 Ländern. Der SVIR wurde 1980 gegründet und zählt rund 2500 Mitglieder aus sämtlichen Branchen.

Die SVIR-Mitglieder resp. Internen Revisoren arbeiten primär mit dem vom IIA erlassenen Standardwerk IPPF (Internationale Standards der Berufspraxis). Das Internal Audit ist sehr oft diejenige Stelle in Unternehmen und Organisationen, welches bezüglich Risiken und deren Management den grössten Überblick hat und deshalb via Verwaltungsrat resp. Audit Committee einen substanziellen Beitrag zur Erhaltung/Erhöhung des Unternehmenswertes leisten kann. Dies stärkt den Berufsstand des Internal Audit und führt zu einer besseren Corporate Governance.

Direkt unterstützen wir Interne Revisoren resp. deren Abteilungen durch entsprechende Aus- und Weiterbildungen (zu aktuellen Themen) sowie Zertifizierungen (CIA, CCSA, CFSA, CGAP, CRMA), beurteilen deren Tätigkeit durch External Quality Assessments und vermitteln ihnen Zugang zu Fachdokumentationen sowie entsprechendem (internationalen) Netzwerk. Die jährliche nationale SVIR-Konferenz ist in der Regel die grösste Plattform für den vielfältigen Austausch. Am 21./22. September 2017 findet an ihrer Stelle erstmals die entsprechende Europäische Konferenz der Internen Revisoren (ECIIA) in der Schweiz, in Basel statt.

ISACA

Die Information Systems Audit and Control Association (ISACA) ist eine weltweite Verbindung von Fachleuten, die sich mit Sicherheit, Kontrolle, Revision und Management von Informationssystemen befassen; sie wurde bereits 1969 gegründet. Die Dachorganisation hat über 200 Chapter in ca. 80 Ländern – mit insgesamt rund 140’000 Mitgliedern aus 180 Ländern. Heute ist ISACA zusammen mit dem IT Governance Institute der Knowledge-Provider für IT Enterprise Governance, Information Systems Audit, Information Security und IT Risk Management. Die ISACA setzt sich in professioneller Art mit allen Entwicklungen in diesen Themenbereichen auseinander, organisiert globale Konferenzen und macht ihre diesbezüglichen Erkenntnisse interessierten Kreisen weltweit zugänglich. Zu den bekanntesten Produkten gehören die international anerkannten Frameworks COBIT®, Val IT™ und Risk IT – und seit ein paar Jahren auch auf "Cybersecurity" spezialisierte Standards.

Das ISACA Switzerland Chapter wurde 1988 als Verein gegründet. Es richtet sich ebenso an Vertreter der internen und externen Revision wie an Spezialisten, welche sich mit Fragen der Informationssicherheit und der Qualitätskontrolle beschäftigen. Die rund 1500 Mitglieder kommen aus den verschiedensten Bereichen, vom Rechnungswesen über die Beratung, die Revision bis hin zur Informationstechnologie – sowie aus verschiedensten Hierarchiestufen der Unternehmen.

Neben verschiedensten Schulungen als Vorbereitung auf die globalen Zertifikatsprüfungen CISA, CISM, CGEIT und CRISC (und neu auch CSX) organisiert das ISACA Switzerland Chapter seit 2003 unter dem Titel "ISACA After Hours Seminare" (AHS) zirka einstündige Vorträge zu aktuellen Themen. Thematisch decken die AHS die Haupttätigkeitsgebiete der ISACA, IT Enterprise Governance, IS Audit, Information Security und Riskmanagement ab.

Die Autoren

Dr. Olga Valek, lic. oec. HSG, CIA befasst sich seit über 20 Jahren in verschiedenen internationalen Funktionen mit den Themen Internal Audit, Risk Management, Corporate Governance sowie dem ganzheitlichen Management. Nun ist sie beim SVIR für die fachliche Weiterentwicklung und Quality Assurance zuständig.

Peter Marti, CISA, im Vorstand des ISACA Switzerland Chapters. Seit 18 Jahren in der Informatik in verschiedensten operativen und strategischen Funktionen. Heute interner IT-Auditor bei der Bank Julius Baer.

(Quelle: ISACA)