Überblick zur Information Security Governance

Sofern die eingesetzte Informationstechnik zielorientiert und unter Einhaltung der Vorgaben aus dem Informationssicherheitsmanagement (im Einklang mit der ISO/IEC 27000er Reihe) gesteuert werden soll, spricht man von einer sog. "**Information Security Governance**". Das IT Governance Institute versteht darunter den Schutz der eigenen Information Assets unter Einhaltung der Informationssicherheit und der Vermeidung vor allem der fortbestandsgefährdenden Risiken (siehe [ITGI2006]).

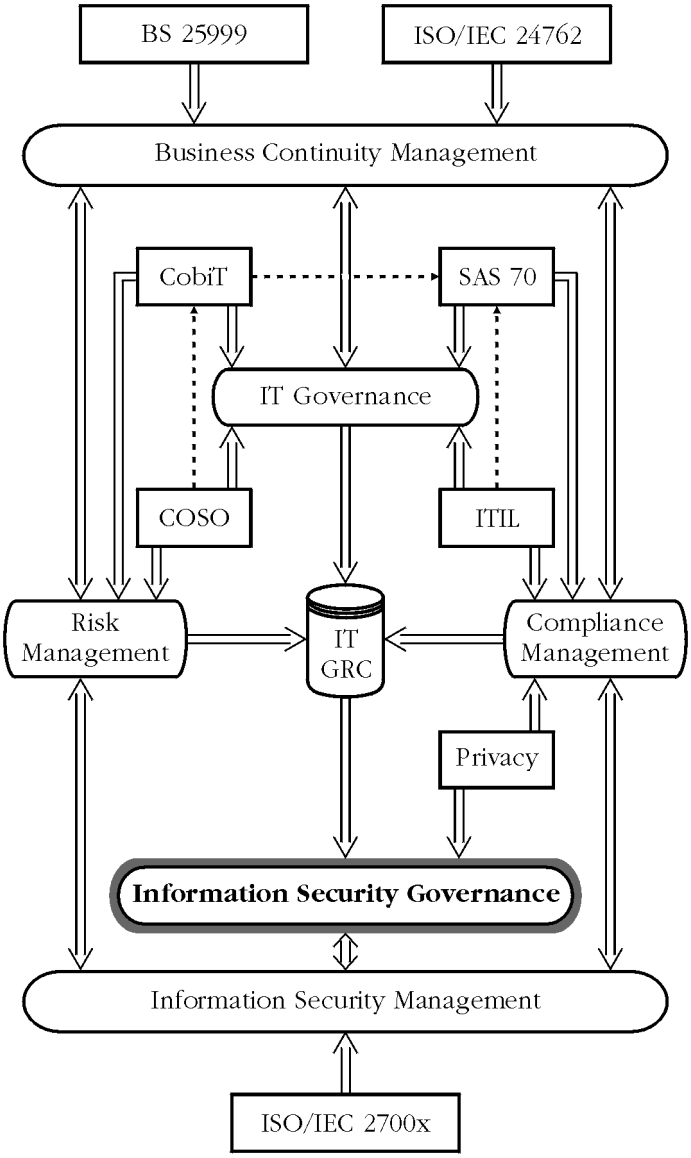
Aufgrund der Verschränkung der Information Security Governance mit anderen Normen wie vor allem zum Disaster Recovery (nach ISO/IEC 24762) und zum Business Continuity Management (nach BS 25999) ist es üblich, einen möglichst hohen Anteil der Tätigkeiten zu automatisieren. Die hierfür verwendete Technik nennt sich "**IT Governance, Risk and Compliance Management System**" und verfolgt folgende Aufgaben (siehe [Witt2008]):

- Die **IT Governance** ist die Steuerung der Informationstechnik in der Weise, dass getroffene Richtlinien, eingestellte Policies und durchgeführte Prozeduren letztlich den Geschäftszweck unterstützen, so dass hier eine hohe Überschneidung mit dem Business Continuity Management gegeben ist (vgl. den entsprechenden Passus im Kapitel "Konzeption von IT-Sicherheit" der Vorlesung zu den "Grundlagen des Datenschutzes und der IT-Sicherheit")
- Das **Risk Management** dient der Vermeidung, der Abmilderung oder dem Transfer fortbestandsgefährdender Risiken (vgl. das entsprechende Kapitel "Risiko-Management" der Vorlesung zu den "Grundlagen des Datenschutzes und der IT-Sicherheit")
- Das **Compliance Management** stellt sicher, dass geltende Gesetze, getroffene Vereinbarungen mit Vertragspartnern (vor allem der SLAs) und der aktuelle Stand der Technik eingehalten werden (vgl. die entsprechenden Ausführungen im Kapitel "Anforderungen zur IT-Sicherheit" der Vorlesung zu den "Grundlagen des Datenschutzes und der IT-Sicherheit" und [Witt2006a], [Witt2006b] und [Witt2007])

In der Praxis wirken auf die entsprechende Gestaltung der IT unter den Vorgaben der Information Security Governance auch **internationale Rahmenwerke** ein wie COSO, CobiT, SAS 70 und ITIL sowie weitere branchenspezifische Standards und natürlich die entsprechenden Anforderungen vor allem aus Sicht des **Datenschutzes** (vgl. vor allem das Kapitel "Technischer Datenschutz" der Vorlesung zu den "Grundlagen des Datenschutzes und der IT-Sicherheit").

Letztlich ist es daher die **Aufgabe** der Information Security Governance, im Rahmen der Steuerung nicht nur die Verlässlichkeit der Informationstechnik (unter Beachtung der Vorgaben aus dem Information Security Management, Disaster Recovery Management und Business Continuity Management), sondern eben auch die Beherrschbarkeit der Informationstechnik sicherzustellen. Daher kann dieser ganzheitliche Ansatz als besonderer Aspekt mehrseitiger IT-Sicherheit angesehen werden (vgl. das Kapitel "Mehrseitige IT-Sicherheit" der Vorlesung zu den "Grundlagen des Datenschutzes und der IT-Sicherheit").

Die verschiedene Bereiche miteinander vernetzende Information Security Governance kann daher wie folgt skizziert werden:



Bernhard C. Witt

Verwendete Quellen:

[ITGI2006] IT Governance Institute: Information Security Governance – Guidance for Boards of Directors and Executive Management. ITGI, Rolling Meadows, 2006, 2nd Edition.

[Witt2006a] Bernhard C. Witt: Rechtssicherheit – Sicherheitsrecht: Rechtliche Anforderungen an die Informations-Sicherheit. <kes> 2006#1, S. 92-96.

[Witt2006b] Bernhard C. Witt: Gewährleistung der Compliance. IT-SICHERHEITpraxis 5/2006, S. 31.

[Witt2007] Bernhard C. Witt: Compliance-Anforderungen durch international Standards. IT-SICHERHEITpraxis 2/2007, S. 30-31.

[Witt2008] Bernhard C. Witt: IT Governance, Risk and Compliance Tools. IT-SICHERHEITpraxis 3/2008, S. 32-33.