IT Governance, Risk & Compliance Management – Praktische Erfahrungen –

Vortrag im Workshop zur Datensicherheit

bei der DGRI-Jahrestagung 2010

am 08.10.2010 in Nürnberg

Bernhard C. Witt

it.sec
security for your information

- Berater für Datenschutz und Informationssicherheit bei der it.sec GmbH & Co. KG
- Industriekaufmann, Diplom-Informatiker
- geprüfter fachkundiger Datenschutzbeauftragter (UDIS)
- Lehrbeauftragter an der Universität Ulm (seit 2005)
- Autor der Bücher „IT-Sicherheit kompakt und verständlich“ (2006) und „Datenschutz kompakt und verständlich“ (2008 & 2010)
- verantwortlich zum Thema Compliance der IT-SICHERHEITpraxis (2006 – 2009)
- Sprecher der GI-Fachgruppe Management von Informationssicherheit
- Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit – Schutz und Zuverlässigkeit

Zur GI-FG SECMGT

Die GI-Fachgruppe **Management von Informationssicherheit**

bietet den im Bereich des Managements von Informationssicherheit tätigen Personen eine neutrale Plattform, um sich miteinander zu vernetzen sowie Wissen und Erfahrungen auszutauschen.

- ist Teil der **Gesellschaft für Informatik** e.V. (gemeinnützige Fachgesellschaft zur Förderung der Informatik)
- besteht seit März 2002 als Teil des Fachbereichs Sicherheit
- vertritt praxisorientierte Themen zu Management, Konzeption, Betrieb und Fortentwicklung von Informationssicherheit
- bietet mind. 2 öffentliche Workshops pro Jahr (Teilnahme kostenfrei)

→ Nähere Informationen unter www.secmgt.de

Zur it.sec GmbH & Co. KG

- beratend tätig zu:
  - Informationssicherheitsmanagement
  - IT-Risikomanagement
  - Business Continuity Management
  - externer Datenschutzbeauftragter bzw. Datenschutzberatung
  - Penetrationstests zu Infrastruktur und Web-Applikationen
  - Firewall-Audits
  - IT-Forensik
  - Planung, Integration und Management von Sicherheitssystemen

  → **Dienstleister ganzheitlicher Informationssicherheit**
- seit 1996 am Markt; mit Standorten in Ulm und München
- bundesweit (mit Schwerpunkt im Süden) beauftragt von: IT-Dienstleister, Industrie, Banken- und Finanzsektor, Steuerberater, Behörden, Gesundheitswesen, Krankenkassen, u.v.a.m.

→ Nähere Informationen unter www.it-sec.de

IT Governance, Risk & Compliance Management

IT Governance → **Steuerung** der IT im Sinne des Geschäftszwecks
- z.B. nach ISO/IEC 38500:2008

IT Risk Management → **Umgang** mit (fortbestandsgefährdenden) Gefährdungen der IT
- z.B. nach ISO/IEC 27005:2008

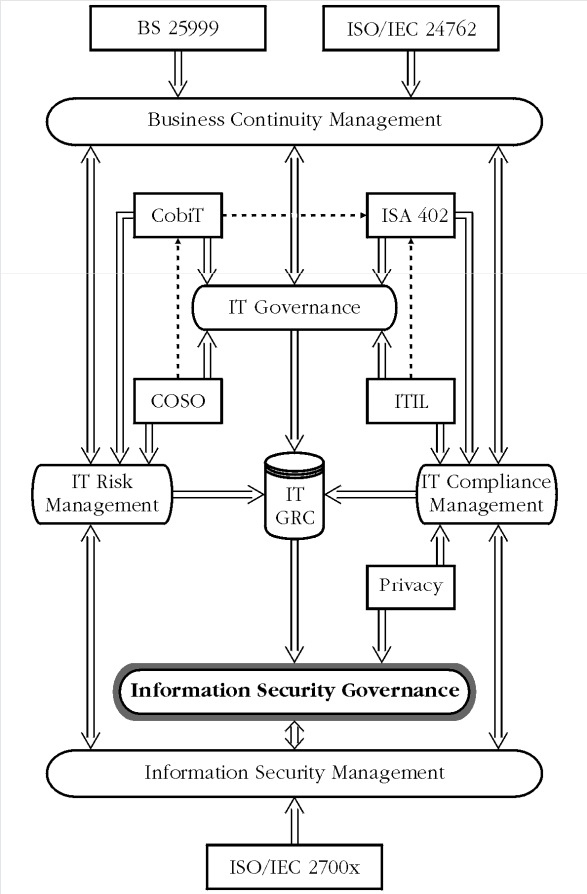
IT Compliance Management → **Einhaltung** geltender Gesetze, getroffener Vereinbarungen und des aktuellen Stands der Technik beim Einsatz der IT

IT-GRC-Management stellt ein grundlegendes Element für das Management von Informationssicherheit dar

Gründe für Einrichtung von IT-GRC Management (1)

- Unübersichtlich viele **regulatorische Anforderungen**:
  - Bereichsrecht
  - Datenschutzrecht
  - Telekommunikationsrecht
  - Telemedienrecht
  - Sorgfaltspflichten
  - Steuer- & Handelsrecht
- **Haftungsbegrenzung** durch Orientierung am „Stand der Technik“
  → internationalem best practice wird hohe Entlastungswirkung zugesprochen
- **Nachweispflichten** für Staat & Vertragspartner
  → diverse Audits verschiedener Stellen (Wirtschaftsprüfer, Aufsichtsbehörden, Vertragspartner, u.a.m.) zu vergleichbarem Inhalt

Gründe für Einrichtung von IT-GRC Management (2)



Die Gewährleistung von IT Governance, Risk & Compliance Management wird beeinflusst durch:

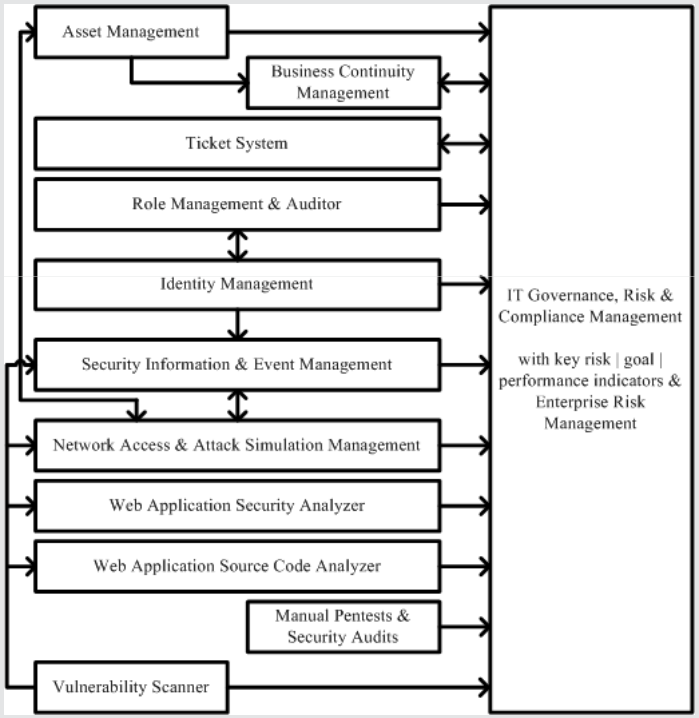
- **Verhinderung fortbestandsgefährdender Risiken**
  - rechtlich gefordert durch KonTraG
  - baucht vorausschauendes Risikomanagement (Erkennung, Bewertung & Umgang mit Risiken) und Business Continuity Management (Kontinuität der Wertschöpfungskette)
  - IT hat darin Schlüsselposition inne
- **Steuerliche Anforderungen** & internationale Verflechtungen
  - Ausrichtung der Finanz-IT im Einklang mit internationalen Frameworks (z.B. wg. SOX)
  - regelmäßige Audits durch verschiedene Stellen

→ **Planvolles Handeln & solide Datenbasis nötig**

Aufbau einer IT-GRC-Infrastruktur

Plan:	
1.	**Specification of Information Security Objectives**
2.	**Identification of Corresponding Protection Requirements**
Do:	
3.	**Modeling of the IT-GRC System**
4.	**Insertion of Organisational Measures in IT-GRC System**
5.	**Combining of the IT-GRC System with Automated Technical Measures**
Check:	
6.	**Performance of Effectiveness Audits & Tests**
7.	**Determination of KRI, KPI & KGI**
Act:	
8.	**Reporting, Remediation of Risks & Monitoring**
9.	**Continual Improvement of the Information Security Governance Infrastructure**

Beispielhaftes Vorgehensmodell



Beispiel-Infrastruktur

Typische Probleme beim IT-GRC-Management (1)

- Einrichtung eines IT-GRC-Managements erfordert umfassenden Prozess & **Zusammenarbeit** vieler verschiedener Stakeholder (& Interessen!)
- Nötige **Datenbasis** schwierig zusammenzutragen:
  - Definition der key risk/performance/goal indicators oft unklar
  - Ermittlung & Klassifizierung der Information Assets (= Prozesse, Informationen, Hardware, Software, Netzwerkkomponenten, Personal, Gebäude, etc.) i.d.R. aufwändig – vor allem hinsichtlich der Granularität
  - Zusammentragen von Daten aus verschiedenen Quellen meist mühsam
- Eine **technische** All-in-One-**Lösung** existiert nicht
  → Kombination verschiedener Instrumente erforderlich
  → Datenaustausch verschiedener IT-Systeme (Log- & Konfigurationsdaten)
  → Zu beachten: Interoperabilität!
- Aussagekraft eines IT-GRC-Managements hängt vor allem von der Eignung der gewählten **Modellierung** ab!

Typische Probleme beim IT-GRC-Management (2)

- **Durchführung** des IT-GRC-Managements unterliegt wiederum selbst rechtlichen Anforderungen:
  - Umgang mit **personenbezogenen Daten** (→ IP-Adressen, User-IDs, Benutzerrollen, virtuelle Datenprofile, …)
  - betriebliche/behördliche **Mitbestimmung**, da z.T. technische Verhaltens-kontrolle mit IT-GRC-Management verbunden
  - **Wirksamkeitstests** seit Einführung des § 202c StGB in der Praxis mit gewisser Unsicherheit verbunden
  - Einbindung **Externer** unter Beachtung des neuen § 11 BDSG
- **Besonderheit** des Rohstoffs „Information“ und allgegenwärtige & ineinander konvergierende Informations- und Kommunikationstechnik bisher nur ein-geschränkt adäquat in Rechtsnormen abgebildet
- Steigende Zahl Wirtschaftsspionagen, Datenpannen & Datenträgerverluste führt teilweise zur „hektischen“ Einführung von IT-GRC-Management (nicht immer **wirtschaftlich** sinnvoll)

Typische Probleme beim IT-GRC-Management (3)

- **Stand der Technik** (= Entwicklungsstand technischer Systeme, der zur vorsorgenden Abwehr spezifischer Gefahren geeignet und der verantwortlichen Stelle zumutbar ist) **unterschiedlich** zwischen den Branchen aufgrund der jeweiligen Rahmenbedingungen (sowie innerhalb einer Branche!)
- Alleine das Vorliegen eines **zertifizierten** Informationssicherheitsmanagementsystems (ISMS), z.B. nach der ISO/IEC 27001, bedeutet nicht, dass dieses sinnvoll gewählt wurde und wirksam ist bzw. im Sinne eines ganzheitlichen IT-GRC-Managements wirken kann
  ° allerdings wird die Chance für positives Resultat merklich erhöht
  ° bei Zertifikaten ist jedoch der angegebene Scope sehr genau zu prüfen
  → u.U. trügerische Sicherheit! (vs. dem Wunsch nach Verbindlichkeit)
- Die Güte eines IT-GRC-Managements ist vor allem davon abhängig, ob das **IT-Risk-Assessment** umfassend (inkl. Outsourcing!) durchgeführt wurde
  → in der Praxis oft anzutreffende „Checklistenorientierung“ sub-optimal
  → mangelnde Verzahnung mit Corporate Risk-Management bedauerlich

Noch Fragen?

Vielen Dank für Ihre Aufmerksamkeit!