Steuerung ganzheitlicher Informationssicherheit
im Rahmen des IT Governance, Risk & Compliance Managements

Abstract:
Die zunehmende Komplexität eingesetzter Informations- und Kommunikationstechnik und die Vielfalt zu berücksichtigender Vorgaben erfordert insbesondere bei Banken ein planvolles Vorgehen. Hierzu bietet sich eine Steuerung ganzheitlicher Informationssicherheit an, die einen toolunterstützten Ansatz verwendet. Beim Aufbau einer entsprechenden Infrastruktur sind die besonderen Anforderungen des Informationssicherheitsmanagements, des Disaster Recovery & Business Continuity Managements und des IT Goverance, Risk and Compliance Managements zu beachten. Daher fungiert konsequenter Weise ein IT GRC Tool als zentrale Einheit einer solchen Infrastruktur. Dieses System sollte dazu in der Lage sein, auch technische Informationen unterschiedlicher Systeme automatisiert einzubeziehen und handlungsvorbereitend zu bewerten. Besonders hilfreich ist eine derartige Infrastruktur, wenn bereits vor Ergreifung einzelner Maßnahmen eine Bestimmung des zu erwartenden Restrisikos erfolgt.

Handout zum Vortrag auf dem it-sa Banken-Symposium am 13. Oktober 2009 von Bernhard C. Witt, it.sec GmbH & Co. KG

Inhalt:

Besondere Anforderungen an Informationssicherheit bei Banken

Die aktuellen Anforderungen an die Gestaltung der eingesetzten Informations- und Kommunikationstechnik (IKT) einer Bank sind hoch und steigen kontinuierlich weiter. So sind beim IKT-Einsatz mittlerweile viele verschiedene Rahmenvorgaben zu beachten: Neben zahlreichen regulatorischen Vorgaben aus Gesetzen (insbesondere zum Banken-, Datenschutz-, Telekommunikations- und Telemedienrecht sowie zur Sorgfalts- und Verkehrssicherungspflicht) oder Vorschriften (z.B. zur manipulationssicheren Archivierung steuerlich relevanter Unterlagen) stehen auch Anforderungen auf der Grundlage der Beziehungen zu Lieferanten, Kunden und Mitarbeitern auf der Agenda (siehe [1]).

Im Zentrum der regulatorischen Anforderungen stehen die operationellen Risiken, wie sie sich aus den Vorgaben zu Basel II und (im Einklang mit der EU-Kreditinstituten-Richtlinie 2006/48/EG) der jeweiligen nationalen Umsetzung in Gesetzen und Regelungen der Bankenaufsicht ergeben. Unter Operationellem Risiko wird die Gefahr von Verlusten verstanden, die infolge einer Unzulänglichkeit oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse eintreten. Welche Maßnahmen daraus folgen, lassen sich an den Grundsätzen für eine wirksame Bankenaufsicht des Basler Ausschusses für Bankenaufsicht und den weiteren Ausführungen in der Methodik der Grundsätze für eine wirksame Bankenaufsicht und in den Praxisempfehlungen für Banken und Bankenaufsicht zum Management operationeller Risiken sowie der deutschen Umsetzung in den MaRisk ablesen. Zudem muss eine Bank den Vorgaben der EU-MiFID-Richtlinie 2004/39/EG über eine ordnungsgemäße Verwaltung und Buchhaltung, interne Kontrollmechanismen, effiziente Verfahren zur Risikobewertung sowie wirksame Kontroll- und Sicherheitsmechanismen für Datenverarbeitungssysteme verfügen.

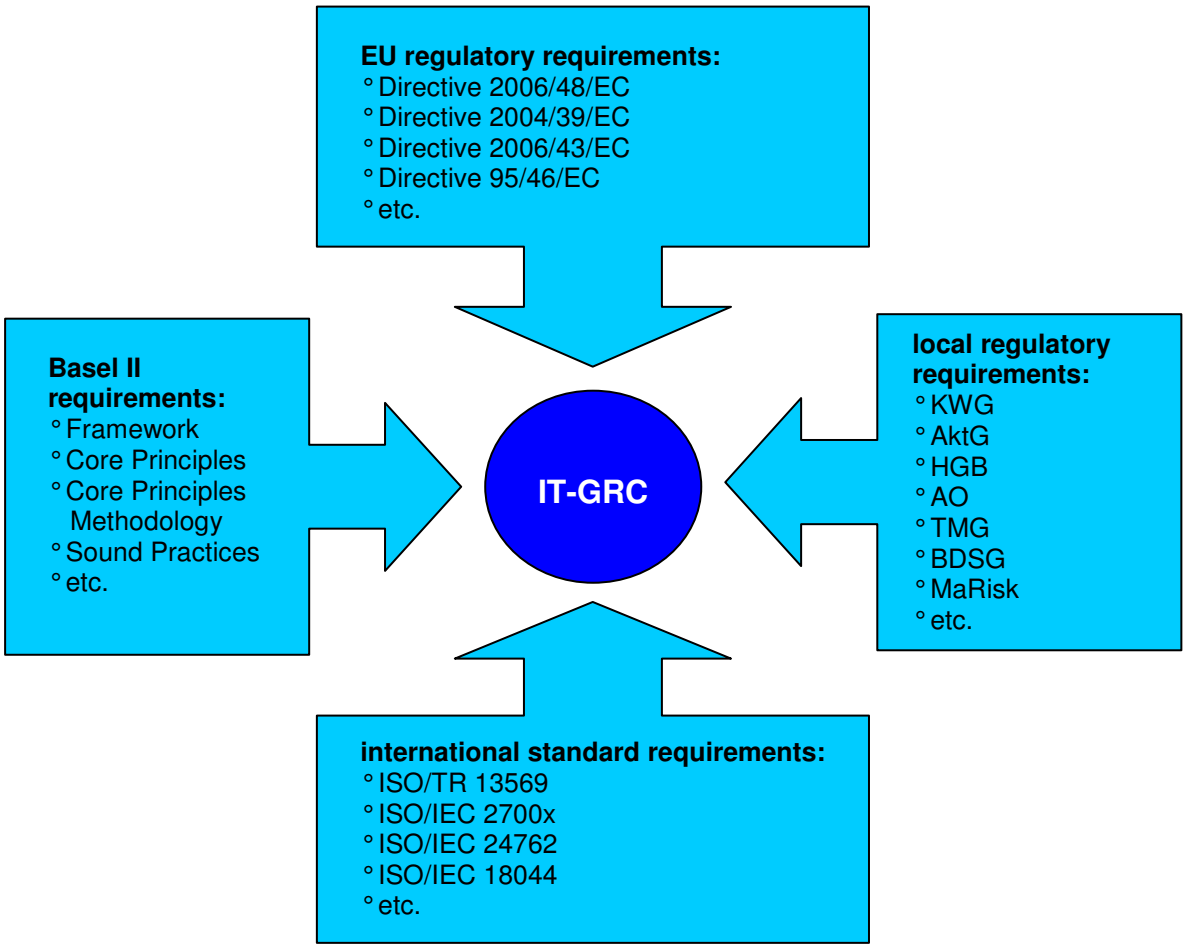

Abbildung 1: Überblick zu regulatorischen Anforderungen für Informationssicherheit bei Banken

Um diese Anforderungen bewältigen zu können, ist ein planvolles Handeln geboten, zu dem diverse Stellen einer Bank einen inhaltlichen Beitrag leisten müssen. Im Sinne einer zielorientierten Steuerung der eingesetzten IKT wird hierbei sinnvollerweise ein ganzheitlicher Ansatzes verfolgt unter der Maßgabe, die eigenen Information Assets wirksam zu schützen und mittels der IKT die bestehenden strategischen Vorgaben unter Einhaltung der Informationssicherheit und der Vermeidung fortbestandsgefährdender Risiken umzusetzen.

Im internationalen Standard ISO/IEC 38500 ist skizziert, welche Aufgaben in diesem Zusammenhang dem Top Management obliegen. Eine inhaltliche Beschreibung, was konkret bei der Umsetzung zu beachten ist, ist für Banken näher in der ISO/TR 13569 ausgeführt, deren Einhaltung zur üblichen Sorgfaltspflicht im Bankensektor zählt, und erfolgt demnach mittels Leitlinien, Policies und zugehörigen Vorgehensweisen. Dies stellt eine wichtige Voraussetzung für ein effektives internes Kontrollsystem (IKS) dar, erzeugt jedoch i.d.R. eine hohe Dokumentationsflut, um entsprechende Nachweise liefern zu können.

compliance with ISO/TR 13569	
• corporate information security policy	
• IT security programme	compliance with requirements
	effective security controls
	adequate disaster recovery
	effective incident management
	comprehensive security monitoring
	IT governance
• risk analysis	
• business impact analysis	
• asset classification scheme	

Abbildung 2: Gewährleistung der Compliance mit der ISO/TR 13569

Aufgrund der sich anlassabhängig unterscheidenden Blickwinkel spezifischer Compliance-Audits, die zunehmend eingefordert werden, sind sowohl hinsichtlich der Vorbereitung als auch der zu erstellenden Dokumentation viele inhaltsgleiche Ausarbeitungen erforderlich, die bisher meist in mühevoller Handarbeit zusammengetragen werden. Dieser Mehraufwand lässt sich stark reduzieren, indem man einen ganzheitlichen Ansatz verfolgt. Idealerweise wird dieser technisch durch weitgehend automatisierte Vorgehensweisen unterstützt und hilft dabei, fortbestandsgefährdende Aktivitäten nachweislich zu vermeiden.

Die neugefassten EU-Vorgaben für den Finanzsektor im Rahmen der EU-Richtlinie 2006/48/EG (Anhang X Teil 3 Nr. 12) fordern für den Fall, dass eine Bank den fortgeschrittenen Messansatz (AMA) verwenden möchte, ausdrücklich ein intern konsistentes Risikomesssystem, das eine Mehrfachzählung von qualitativen Bewertungen oder Risikominderungstechniken, die bereits in anderen Bereichen des Kapitaladäquanzrahmens anerkannt werden, ausschließt. Hinsichtlich der alle Bereiche durchdringenden IKT erfordert dies eine sinnvolle Modellierung und Dokumentation.

Umsetzungsstrategie einer ganzheitlichen Information Security Governance

Auf Basis realer Projekte (und der zusätzlichen Ausführungen zur Architektur einer entsprechenden Infrastruktur unter [2]) kann beispielhaft gezeigt werden, wie insbesondere bei Banken eine toolunterstützte Steuerung ganzheitlicher Informationssicherheit erreicht werden kann. Trotz der damit verbundenen Gestehungskosten ist der Aufbau einer vollständigen Information Security Governance Infrastruktur bei Banken durchaus angezeigt. Damit wird nachweislich der Stand der Technik gewährleistet, der (branchenspezifisch) zur vorsorgenden Gefahrenabwehr geeignet und der Bank auch zugemutet werden kann. Es kann aber bereits mit einer, lediglich einzelne Teile betreffenden Umsetzung schon Einiges erreicht werden, insbesondere wenn ein sukzessiver Ausbau in die skizzierte Richtung vorgesehen ist.

Im Rahmen der Steuerung ganzheitlicher Informationssicherheit sollte der eigene Ist-Stand so aktuell wie möglich darstellbar sein – sowohl bezüglich der Sicherheitslage und bestehender IT-Risiken als auch des Compliance-Erfüllungsgrades und bei der Unterstützung der Wertschöpfungskette durch die IKT – (z.B. durch Auswahl eines geeigneten Dashboards) und im Branchenvergleich (z.B. im Sinne eines Benchmarkings). Dies setzt die Normalisierung verarbeiteter Daten sowie die Verwendung vergleichbarer Metriken (vor allem hinsichtlich der Key Risk Indicators, Key Goal Indicators und Key Performance Indicators) voraus.

Als ein Echtzeit-Lieferant derartiger Daten kann ein Security Information and Event Management System (SIEM) fungieren; doch dies alleine ermöglicht noch keine Steuerung ganzheitlicher Informationssicherheit! Zentraler Aspekt der Steuerung ist schließlich, nicht nur nachträglich festzustellen, welches Sicherheitsniveau in Anbetracht vorliegender Schwachstellen erreicht wurde, sondern auch potenzielle Auswirkungen vorgesehener Änderungen vorab abschätzen zu können.

Um Synergien bei der ganzheitlichen Information Security Governance nutzen zu können, bedarf es einer Lösung, die zentrale Managementebenen mit Vorgehensweisen zur Umsetzung relevanter Normen verknüpft. Insofern sind neben der IT Governance auch das Risk Management und das Compliance Management als wesentliche Bausteine einer Information Security Governance anzusehen!

Der jeweilige Umfang der zugehörigen Kernfunktionen ist enorm und die Übersicht kann recht schnell verloren gehen. Bei der Bewertung der eigenen Sicherheitslage ist es hilfreich, über eine aktuelle Datenbasis zu verfügen, was mit den klassischen, interviewgestützten Erhebungen kaum sinnvoll erreicht werden kann. Deshalb ist der Einsatz eines IT Governance, Risk and Compliance (GRC) Tools sinnvoll, welches in der Lage ist, automatisiert erhobene Daten zu verarbeiten und auf relevante Controls anzuwenden (siehe auch [3]).

Außerdem überlappen sich faktisch viele Controls unterschiedlicher Standards inhaltlich, was aber gerade geeignete IT GRC Tools durch sogenanntes „Cross-Control-Mapping" zwischen verschiedenen Frameworks aufzeigen und optimieren können – als Beispiel mögen die in nahezu jedem Framework vorkommenden „Access Controls pro Asset" dienen. Viele IKT-Systeme werden in der Praxis zur Umsetzung verschiedener Aufgaben verwendet und unterliegen dadurch differierenden Anforderungen sowohl rechtlicher Natur als auch hinsichtlich der relevanten Standards und Frameworks. Bisher müssen dann im Rahmen von Audits (und den zugehörigen Vorbereitungen) inhaltsgleiche Fragen mehrfach beantwortet und verwaltet werden. „Cross-Control-Mapping" eliminiert diesen Mehraufwand.

Gängige IT GRC Tools verfügen über eine managementtaugliche Aufbereitung mittels sog. Dashboards, die einen schnellen Überblick verschaffen helfen, und sind beim Monitoring behilflich. Des Weiteren berücksichtigen aktuelle IT GRC Tools Vorgaben internationaler Standards zum Disaster Recovery Management (ISO/IEC 24762) und Business Continuity Management (BS 25999), sodass sich im Rahmen der Steuerung eine langfristige Wirkung entfalten kann (zu den Prüfkriterien einer geregelten Datensicherung siehe [4]).

Aufbau einer toolunterstützten Information Security Governance

Eine All-in-One-Lösung, die alle Anforderungen bündelt und quasi per Mausklick Hinweise für durchzuführende technische und organisatorische Maßnahmen ausgibt, um jegliche Organhaftung wirksam ausschließen zu können, gibt es nicht und wird es vermutlich auch nie geben. Allerdings lässt sich in der Kombination besonders geeigneter Tools eine ganzheitliche Sichtweise auf komfortable Weise unterstützen. Eine Herausforderung bei der Auswahl der miteinander zu diesem Zweck zu kombinierenden Tools ist nicht zuletzt, die Interoperabilität beim Datenaustausch zu gewährleisten!

Der beim Aufbau einer geeigneten Information Security Governance Infrastruktur zur Anwendung kommende Prozess lässt sich im Einklang mit dem bewährten Deming Cycle hinsichtlich der Hauptaktivitäten wie folgt skizzieren:

Plan:

1. Festlegung der einzuhaltenden Sicherheitsziele, die gerade bei Banken in einzelnen Bereichen auch über die Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit hinaus gehen, um z.B. die Authentizität und Nichtabstreitbarkeit von Aktionen nachweisen zu können – hier liefern internationale Standards wie z.B. die ISO/IEC 27001 eine strukturierte Vorgabe
2. Bestimmung der zu schützenden Information Assets (inkl. der Abhängigkeiten und des Zusammenschlusses von Assets zu einem Verbund) und deren Kritikalität sowie Wertigkeit – dabei ist der Schutzbedarf ausschlaggebend und datenschutzrechtliche Anforderungen zu berücksichtigen

Do:

3. Anwenden der festgelegten Sicherheitsziele auf die Gestaltung und Verwendung der Information Assets – dies erfordert eine umfangreiche Modellierung und geschieht zweckmäßigerweise unter Beachtung internationaler Standards zur Datensicherung nach ISO/IEC 24762 und BS 25999 sowie zur Gestaltung von IT-Services nach ITIL bzw. CobiT und bei einem Outsourcing finanzwirksamer IT-Dienstleistungen nach SAS 70, was von IT GRC Tools unterstützt wird, welche entsprechende Content Packages aufweisen
4. Zusammentragen relevanter organisatorischer Anweisungen und deren (i.d.R. checklistenartige) Abbildung im Rahmen des IT GRC Tools – ein entsprechender Transfer papierner Regeln und technischer Parametereinstellungen in entsprechende Tools erfordert i.d.R. erhebliche Anpassungsarbeiten

5. Zusammentragen technischer Basisdaten (automatisiert!) im IT GRC Tool – dabei ist darauf zu achten, dass die eingesetzten Tools eine einheitliche "Sprache" sprechen und vergleichbare Ergebnisse liefern.

Check:

6. Durchführung ergänzender Audits und automatisierter Tests (ggf. unter Berücksichtigung fallbasierter Alternativen) zur Abrundung und Kontrolle des Ist-Standes – dies dient als Beleg für die Wirksamkeit des verwendeten Rahmenwerks und damit der Haftungsentlastung
7. Bewertung der Ergebnisse unter Zuhilfenahme bereitgestellter Metriken (Key Risk / Goal / Performance Indicators) des IT GRC Tools – unter dem besonderen Fokus auf eine ganzheitliche Sicht

Act:

8. Report der Bewertung, Beheben festgestellter Mängel und Monitoring der Langzeitentwicklung – die eingesetzte Infrastruktur sollte hierzu möglichst zeitnahe Berichte "auf Knopfdruck" liefern
9. Anpassung der bestehenden Information Security Governance Infrastruktur und ggf. geeignete Modifikation von deren Konfiguration – im Rahmen der kontinuierlichen Fortentwicklung

Beim Aufbau einer Information Security Governance Infrastruktur sollte man darauf achten, dass Ergebnisse sicherheitsrelevanter IKT-Bereiche an der jeweiligen Stelle sinnvoll abgerufen und mit einem einheitlichen Bewertungsschema aufbereitet werden. Die Bündelung erfolgt letztlich durch das IT GRC Tool und dient dem Zweck, dass die Leitungsebene des Unternehmens bzw. der Behörde die nötigen Entscheidungen auf einer soliden Grundlage treffen kann. Durch Inbetriebnahme einer umfassenden Information Security Governance Infrastruktur wurden in der Praxis bereits erhebliche Einsparungseffekte erzielt: Diese ergeben sich einerseits aus deutlich reduzierten Aufwendungen im Rahmen „multiregulatorischer" Audits und Self-Assessments durch die zentrale Verwaltung von GRC-relevanten Assets, die automatische Erfassung Control-relevanter Parameter und schon alleine durch das „Cross-Control Mapping". Weitere Kostenreduktionen ergeben sich aus Fehlervermeidung, frühzeitiger Risikoerkennung und effizienterer Adressierung (wirklich) relevanter Bedrohungen im Rahmen der Priorisierung über IT-Risiken.

Literatur

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

[2] Bernhard C. Witt & Holger Heimann, Tool-Verbund für GRC und Sicherheit – Ansatz zur toolunterstützten Steuerung ganzheitlicher Informationssicherheit, <kes> 2009#2, S. 72ff.

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

[4] Bernhard C. Witt, Datensicherung und Wiederherstellung, IT-SICHERHEITpraxis 6/2008, S. 27f.

Zum Autor:

Dipl.-Inf. **Bernhard C. Witt** ist Berater für Datenschutz und IT-Sicherheit bei der it.sec GmbH & Co. KG, geprüfter fachkundiger Datenschutzbeauftragter (zertifiziert von der Ulmer Akademie für Datenschutz und IT-Sicherheit gGmbH), aktives Mitglied in der Gesellschaft für Informatik (GI), der Gesellschaft für Datenschutz und Datensicherung (GDD) und dem Berufsverband der Datenschutzbeauftragten Deutschlands (BvD), Sprecher der GI-Fachgruppe „Management von Informationssicherheit", Mitglied im Leitungsgremium des GI-Fachbereichs Sicherheit, von 2006 bis 2009 Verantwortlicher zum Thema Compliance der IT-SICHERHEIT praxis, Autor der Bücher „IT-Sicherheit kompakt und verständlich" (2006) und „Datenschutz kompakt und verständlich" (2008) neben zahlreichen Fachartikeln zu Datenschutz, Informationssicherheit und Compliance in <kes> und IT-SICHERHEITpraxis sowie seit 2005 Lehrbeauftragter für Datenschutz und IT-Sicherheit an der Universität Ulm.

it.sec
security for your information

Kontaktdaten:
Tel: +49 (0) 731 / 20589-11
Mail: bernhard.witt@it-sec.de
Fax: +49 (0) 731 / 20589-29