Ganzheitliche Informationssicherheit bei Banken

Bernhard C. Witt

it.sec GmbH & Co. KG
bcwitt@it-sec.de

Zusammenfassung

Damit eine Bank sicherstellen kann, dass sie die immer zahlreicher werdenden Anforderungen zur Informationssicherheit erfüllt, ist eine toolgestützte Steuerung ganzheitlicher Informationssicherheit nötig. Im Zentrum steht dabei das IT Goverance, Risk and Compliance Management. Aufgrund der hohen Anforderungsdichte ist ein sog. „Cross-Control-Mapping“ unverzichtbar. Zu lösende Herausforderungen bestehen nicht nur hinsichtlich der genauen Bestimmung der wichtigsten Inputfaktoren, sondern auch hinsichtlich der Regelungen für den Betrieb eines derartigen Systems. Entscheidend für die Güte des Systems ist, ob das IT Risk Assessment umfassend und zielgenau durchgeführt wird und ob aufgrund der gewählten Modellierung durch Orientierung an internationalen Best Practice Standards zugleich die gewünschte Haftungsentlastung möglich ist.

1 Allgemeine Anforderungen

Viele Institutionen, insbesondere Banken, müssen **zunehmend mehr regulatorische Vorgaben** zur Gestaltung eingesetzter Informations- und Kommunikationstechnik (IKT) beachten. Die einzuhaltenden Gesetze (u.a. zum jeweiligen Bereichsrecht, zum Datenschutz-, Telekommunikations- und Telemedienrecht sowie zur Sorgfalts- und Verkehrssicherungspflicht) und besonderen Vorschriften (wie etwa zur manipulationssicheren Archivierung steuerlich relevanter Unterlagen) werden für Anwender immer unübersichtlicher. Bei den haftungsrechtlichen Gesichtspunkten sind darüber hinaus auch die bestehenden Beziehungen zu Lieferanten, Kunden und Beschäftigten relevant.

Aus diesen Gründen ist es für die Leitungsebene einer Institution von erheblichem Interesse, in Sachen der **Organhaftung** eine Entlastung herbeiführen zu können, zumal in den letzten Jahren von den Gerichten Vorstände und Aufsichtsräte ausdrücklich für unzureichende Sorgfalt in Haftung genommen wurden (siehe insbesondere die Urteile des BGH vom 22.02.2011, Az.: II ZR 146/09, und vom 20.09.2011, Az.: II ZR 234/09).

Gemeinhin wird eine haftungsentlastende Wirkung erwartet, wenn man sich am aktuellen **Stand der Technik** orientiert, welcher wiederum höhere Anforderungen stellt als „allgemein anerkannte Regeln der Technik“ (siehe [Seib13], S. 3003). Deshalb sind normierte Standards an sich noch keine Garantie zur Haftungsentlastung. Unter dem Rechtsbegriff "Stand der Technik" wird der Entwicklungsstand technischer Systeme verstanden, der zur (vorsorgenden) Abwehr spezifischer Gefahren geeignet und der verantwortlichen Stelle auch zumutbar ist (siehe [Marb79], S. 158ff).

P. Schartner · P. Lipp (Hrsg.) · D•A•CH Security 2014 · syssec (2014) 215-226.

International anerkannten **Best Practice Standards** wird in diesem Sinne eine ausreichende Haftungsentlastungswirkung zugesprochen: Die Orientierung an bester Praxis (im Gegensatz zu lediglich "guter Praxis") gleicht insoweit die jedem Standard inne wohnende Ungewissheit ob seiner Aktualität, Effektivität und fallbezogenen Zielgenauigkeit aus (siehe [Witt10], S. 67ff).

Im Zusammenhang mit Fragen zum Umgang mit potenziellen IT-Risiken sind hier hinsichtlich der Normen vor allem die Reihe der ISO/IEC 2700x (und daraus die ISO/IEC 27000, ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27003, ISO/IEC 27005, ISO/IEC 27013, ISO/IEC 27014, ISO/IEC 27031, ISO/IEC 27035 und ISO/IEC 27036-x) sowie hinsichtlich der Frameworks ITIL (v3), CobiT (v5) und COSO I und II relevant. Eine Orientierung an diesen internationalen Standards erfordert alleine aufgrund der Vielzahl der damit verbundenen Regelungserfordernisse allerdings ein planvolles Handeln.

Im Rahmen diverser Audits (durch Wirtschaftsprüfer, Aufsichtsbehörden, Vertragspartner, u.a.m.) muss ein Unternehmen bzw. eine Behörde zudem **zahlreiche Nachweise** erbringen und dabei oft gleichartige Inhalte für verschiedenartige Prüfkataloge prüfergerecht aufbereiten. Gerade in Branchen, die stark reglementiert sind (wie z.B. bei Banken oder im Gesundheitswesen), verursachen "multiregulative" Audits daher erhebliche Kosten.

2 Besondere Anforderungen bei Banken

Im Zentrum der regulatorischen Anforderungen stehen bei Banken neben den allgemeinen Anforderungen an Informationssicherheit die **operationellen Risiken**, wie sie sich aus den Vorgaben zu Basel III 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 hierbei die Gefahr des Eintritts von Verlusten infolge von Unzulänglichkeiten oder des Versagens von internen Verfahren, Menschen und Systemen oder infolge externer Ereignisse verstanden.

In Deutschland muss eine Bank nach § 25a Abs. 1 KWG über eine ordnungsgemäße Geschäftsorganisation verfügen, die insbesondere ein angemessenes und wirksames **Risikomanagement** umfasst. Dies ist regelmäßig zu überprüfen. Zudem muss eine Bank über ein angemessenes Notfallkonzept verfügen, das auch Sicherheitsvorfälle und Ausfälle der IT-Systeme adressiert. Die Ausgestaltung des hierzu eingerichteten Risikomanagements hängt wiederum von Art, Umfang, Komplexität und Risikogehalt der Geschäftstätigkeit ab. Für wesentliche Auslagerungen von Aktivitäten und Prozessen sind schließlich nach § 25a Abs. 2 KWG angemessene Vorkehrungen zu treffen, um übermäßige, zusätzliche operationelle Risiken vermeiden zu können.

Welche Maßnahmen daraus folgen, lässt sich an den „Grundsätzen für eine wirksame Bankenaufsicht“ des Basler Ausschusses für Bankenaufsicht (siehe [BCBS12]) und weiteren Ausführungen dieses Gremiums zu Operationellen Risiken sowie der deutschen Umsetzung in den am 14.12.2012 novellierten **MaRisk** ablesen. Hinsichtlich der technisch-organisatorischen Ausstattung nach AT 7.2 der MaRisk ist in diesem Zusammenhang gemäß den erläuternden Ausführungen der BaFin vor allem auf den IT-Grundschutz-Katalogen des BSI oder auf die ISO/IEC 2700x abzustellen.

Zudem muss eine Bank nach 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.

Die EU-Vorgaben für den Finanzsektor im Rahmen der EU-Richtlinie 2006/48/EG (Anhang X Teil 3 Nr. 12) erfordern bei der Verwendung des **fortgeschrittenen Messansatzes** (AMA) ausdrücklich ein konsistentes Risikomesssystem. Dieses Risikomesssystem muss eine Mehrfachzählung von qualitativen Bewertungen oder den Einsatz von Risikominderungstechniken ausschließen, die bereits in anderen Bereichen des Kapitaladäquanzrahmens anerkannt werden. Der AMA ist für Banken von starkem Interesse, weil eine Erfüllung des AMA zur Folge hat, dass erheblich weniger Eigenkapital zur Risikoabdeckung bereitgehalten werden muss. Hinsichtlich der alle Bereiche durchdringenden IKT erfordert die Verwendung des AMA eine sinnvolle Modellierung und Dokumentation. Dies kann im Allgemeinen durch Aufbau eines IT-Governance, Risk & Compliance Managements erreicht werden.

3 Umsetzung der Anforderungen bei Banken

IT Governance, Risk & Compliance Management (IT GRC Management) setzt sich aus drei Teilaspekten zusammen:

- Unter **IT Governance** ist die auf den unternehmensbezogenen Geschäftszweck ausgerichtete Steuerung der IKT zu verstehen. Hierbei wird auch überprüft, ob bestehende Steuerungsvorgaben durch die geltenden Organisationsrichtlinien (Richtlinien, Policies, Betriebsvereinbarungen, Dienstanweisungen und Prozesse) adäquat umgesetzt werden. Der IT kommt im Rahmen von Corporate Governance faktisch eine Schlüsselposition zu. In diesem Zusammenhang spielen ISO/IEC 27014, CobiT (v5) und COSO I eine zentrale Rolle.
- Beim **IT Risk Management** wird wiederum sichergestellt, dass vor allem die fortbestandsgefährdenden IT-Risiken erkannt und deshalb vermieden, modifiziert, beibehalten oder mit Anderen geteilt werden können. Zur Erkennung, zur Bewertung und zum Umgang mit IT-Risiken ist ein vorausschauendes IT-Risikomanagement unter Beachtung des KonTraG und ein wirksames, an der Wertschöpfungskette ausgerichtetes Business Continuity Management nach ISO 22301 und ISO 22313 nötig. Hinsichtlich des IT-Risikomanagements spielen ISO 31000, ISO/TR 31004, ISO/IEC 27005 und COSO II eine zentrale Rolle.
- Das **IT Compliance Management** gewährleistet schließlich, dass geltende Gesetze, getroffene Vereinbarungen (sowohl mit Dritten als auch hinsichtlich der eigenen Organisationsrichtlinien) und der aktuelle Stand der Technik eingehalten werden (Regelkonformität). Hier wird üblicherweise auch berücksichtigt, nach welchen Kriterien Wirtschaftsprüfer vorgehen (i.d.R. nach dem Prüfstandard ISA 402, in Deutschland als IDW PS 331 umgesetzt, bzw. nach dem Prüfstandard ISAE 3402 und SSAE 16, in Deutschland als IDW PS 951 n.F. umgesetzt).

3.1 IT GRC Management: Umsetzungsstrategie

Ein für eine Bank geeignetes IT GRC Management umfasst stets ein **Informationssicherheitsmanagement**. Um Informationssicherheit in der Praxis ganzheitlich betreiben und steuern zu können, ist eine geeignete Toolunterstützung unerlässlich. Informationssicherheit bindet jedoch erhebliche personelle und finanzielle Ressourcen und muss daher effizient ausgerichtet werden. Es kann bereits mit einer lediglich einzelne Teile betreffenden Umsetzung schon Einiges in der Praxis erreicht werden.

Bei der Einrichtung eines IT GRC Managements wird üblicherweise sehr viel Wert darauf gelegt, dass die Bank einen komfortablen Überblick über den eigenen **Ist-Stand zur IT-Sicherheitslage**, zu bestehenden IT-Risiken und zum Compliance-Erfüllungsgrad erhält. Zudem wünscht sich eine Bank Angaben darüber, wie man im Branchenvergleich abschneidet (z.B. im Sinne eines Benchmarkings). Schließlich möchte eine Bank das zugehörige Datenmaterial nicht erst durch aufwändige Interviews und Audits ermitteln.

Erfahrungsgemäß überlappen sich zahlreiche Controls aus den unterschiedlichen Standards und Frameworks inhaltlich zu einem erheblichen Teil. Das wird von einem geeigneten IT GRC Tool durch sogenanntes „**Cross-Control-Mapping**“ aufgezeigt. Als typisches Beispiel für solche überlappenden Controls mögen die in praktisch allen Standards und Frameworks vorkommenden „Access Controls pro Asset“ dienen.

Viele IKT-Systeme werden in der Praxis zudem zur Umsetzung verschiedener Aufgaben verwendet und unterliegen dadurch **unterschiedlichen Anforderungen** sowohl rechtlicher Natur als auch hinsichtlich der relevanten Standards und Frameworks. Im Rahmen von Audits (und den zugehörigen Vorbereitungen) müssen aus diesen Gründen inhaltsgleiche Fragen gleich mehrfach (ggf. mit leicht unterschiedlicher Ausprägung) beantwortet und anschließend verwaltet werden (zu den sich daraus ergebenden Belastungen siehe auch [Witt12], S. 6ff). „Cross-Control-Mapping“ reduziert diesen Mehraufwand erheblich.

3.2 IT GRC Management: Umsetzungsschritte

Der beim Aufbau einer geeigneten **IT GRC Infrastruktur** zur Anwendung kommende Prozess lässt sich im Einklang mit dem bewährten Deming Cycle (Plan, Do, Check, Act) hinsichtlich der Hauptaktivitäten wie folgt skizzieren (weitere Details siehe [WiHe09], S. 74):

Plan:

1. Festlegung der einzuhaltenden Sicherheitsziele
   Die Sicherheitsziele können und werden gerade bei Banken in einzelnen Bereichen auch über die Gewährleistung der Verfügbarkeit, Integrität und Vertraulichkeit alleine schon aufgrund der Anforderungen aus Basel III hinaus gehen, um z.B. bei Online-Banking die Authentizität und Nichtabstreitbarkeit von Transaktionen nachweisen zu können. Hier liefern internationale Standards wie z.B. ISO/IEC 27001 eine strukturierte Vorgabe, ergänzt um Festlegungen aus ISO/TR 13569 bzw. ISO/IEC TR 27015. Da diese beiden Guidelines, die sich mit dem Management von Informationssicherheit im Bankensektor beschäftigen, bisher noch nicht aufeinander abgestimmt wurden, ist eine intelligente Modellierung nötig.
2. Bestimmung der zu schützenden Primary Assets
   Zu den Primary Assets zählen Informationen (inkl. personenbezogener Daten) und Prozessbeschreibungen (inkl. notwendiger Compliance-Prozesse). Zu diesen Assets werden Angaben benötigt über deren Kritikalität sowie Wertigkeit.
3. Bestimmung der eingesetzten Supporting Assets
   Damit die Primary Assets wirksam geschützt werden können, muss eine Übersicht vorliegen zu den eingesetzten Supporting Assets wie Hardware, Software, Netzwerkkomponenten, Personal, Gebäude, Räume und organisatorische Strukturen (und der jeweiligen Abhängigkeiten der Assets untereinander). Deren Schutzbedarf leitet sich aus den Primary Assets ab, die durch diese Supporting Assets unterstützt werden.

Do:

4. Anwenden der festgelegten Sicherheitsziele auf die Gestaltung und Verwendung der Primary Assets
   Das Anwenden geschieht zweckmäßigerweise unter Beachtung internationaler Standards zur Datensicherung nach ISO/IEC 27031, ISO 22301 und ISO 22313 sowie zur Gestaltung von IT-Services nach ITIL (v3) i.V.m. ISO/IEC 27013 bzw. CobiT (v5) und beim Outsourcing unter Berücksichtigung der ISO/IEC 27036-x. Dies wird üblicherweise von IT GRC Tools unterstützt, welche entsprechende Content Packages aufweisen.
5. Zusammentragen relevanter Organisationsrichtlinien
   Die üblicherweise in hoher Vielfalt bei Banken vorhandenen Organisationsrichtlinien nach AT 5 der MaRisk müssen im Zuge ihrer Einbindung in die IT GRC Infrastruktur i.d.R. erst in eine geeignete (i.d.R. checklistenartige) Abbildung überführt werden. Ein entsprechender Transfer organisatorischer Regeln, welche meist appellartig und nicht unmittelbar in abprüfbarem Format formuliert sind, und technischer Parametereinstellungen in entsprechende Tools sowie die permanente Aktualisierung der Einträge bei Änderung der Organisationsrichtlinien erfordert oft einen erheblichen Aufwand.
6. Zusammentragen technischer Basisdaten
   Automatisiert sind technische Basisdaten (wie insbesondere Konfigurationsdaten) der eingesetzten technischen Supporting Assets ins IT GRC Tool einzuspeisen. Dabei ist darauf zu achten, dass die eingesetzten Tools eine einheitliche "Sprache" sprechen, um einen interoperabler Datenaustausch zu ermöglichen und vergleichbare Ergebnisse liefern zu können. Daher zählt die Normierung von Datenformaten und die Harmonisierung von Schnittstellen zu den hierzu zu bewältigenden (und mit hohem Aufwand verbundenen) Aufgaben.

Check:

7. Durchführung ergänzender Audits und automatisierter Tests
   Um die Wirksamkeit der umgesetzten Maßnahmen innerhalb des IT GRC Tools bewerten zu können, sind ergänzende, i.d.R. semi-automatisierbare Prüfungen durchzuführen. Deren Ergebnisse sind ins IT GRC Tool einzuspeisen. Zusammen mit den automatisierten Prüfungen (durch Abgleich technischer Basisdaten mit Vorgaben aus dem umzusetzenden Regelwerk) dient dies als Beleg für die Wirksamkeit des verwendeten Rahmenwerks und damit der Haftungsentlastung.
8. Bewertung der Ergebnisse
   Unter Zuhilfenahme bereitgestellter Metriken (Key Risk / Goal / Performance Indicators) des IT GRC Tools sind schließlich die festgestellten Ergebnisse zu bewerten. Dies erfolgt aus ganzheitlicher Sicht. Hierbei wird insbesondere dargestellt, welchen Einfluss die aktuelle Ist-Lage auf die Primary Assets hat.

Act:

9. Report der Bewertungen, Beheben festgestellter Mängel und Monitoring der Langzeitentwicklung
   Die eingesetzte IT GRC Infrastruktur sollte hierzu möglichst zeitnahe Berichte "auf Knopfdruck" liefern. Diese müssen sowohl managementtauglich sein (Überblick zur Steuerung) als auch dem technischen Personal eine klaren Hinweis zur Mängelbeseitigung bzw. Administration liefern.

10. Anpassung der bestehenden IT GRC Infrastruktur
    Die eingesetzte IT GRC Infrastruktur benötigt ständige Wartung und Fortentwicklung.

3.3 Herausforderungen

3.3.1 Aufbau einer geeigneten IT GRC Infrastruktur

Der Aufbau einer geeigneten IT GRC Infrastruktur stellt in der Praxis allerdings einige Herausforderungen bereit (siehe auch [Witt10], S. 70f):

- Zum einen müssen bei der Einrichtung eines IT GRC Managements viele verschiedene Stakeholder zusammenarbeiten und deren jeweilige Interessen geeignet ausgeglichen werden. Dies erfordert einen umfassenden und von der Leitungsebene ausdrücklich getragenen Prozess.
- Zum anderen bildet schon die Vereinbarung der zu überwachenden Key Risk / Performance / Goal Indicators und die geeignete Festlegung der zu schützenden Assets vor allem hinsichtlich der zu wählenden Granularität eine hohe praktische Hürde.
- Schließlich ist bei der Auswahl der miteinander zu kombinierenden Tools und IT-Systeme – gerade, wenn Daten automatisiert in das IT GRC Management integriert werden sollen – die Interoperabilität des Datenaustauschs zu gewährleisten. Da nicht alle beteiligten IT-Systeme zwingend die gleiche "Sprache sprechen", kann dieses umfassende Konvertierungsarbeiten nach sich ziehen.

3.3.2 Anforderungen zur Durchführung des IT GRC Managements

Die Durchführung des IT GRC Managements selbst unterliegt wiederum rechtlichen Anforderungen:

- Der im Rahmen des IT GRC Managements erfolgende Umgang mit personenbezogenen Daten muss **datenschutzrechtlichen Anforderungen** genügen. Im Bereich des IT GRC Managements werden zahlreiche personenbezogene bzw. personenbeziehbare Daten automatisiert verarbeitet: IP-Adressen, User-IDs, Benutzerrollen, virtuelle Datenprofile, u.v.a.m.
- Teilweise resultiert aus dem IT GRC Management eine technisch motivierte Verhaltenskontrolle (vor allem, wenn ein potenzieller Verstoß gegen Sicherheitsvorgaben automatisiert Warnmeldungen auslösen soll, die an zuständige Stellen systembedingt weitergeleitet werden sollen). Das unterliegt daher sowohl der datenschutzrechtlichen Vorabkontrolle als auch der **Mitbestimmung**.
- Die bei der Einführung des § 202c StGB in der Praxis zu spürende Unsicherheit für die Verwendung von **Sicherheitstools** ist erst nach den Klarstellungen des Bundesverfassungsgerichts gewichen. Für Wirksamkeitstests eingesetzte Tools bestehen aus diesen Gründen besondere Schutzvorkehrungen und deren konkreter Einsatz ist ausreichend zu dokumentieren.
- Sofern **Externe** bei Aufbau, Unterstützung oder Betrieb des IT GRC Managements beteiligt sind, was in der Praxis eher der Regelfall ist, sind die seit 2009 umfassender gefassten Vorschriften aus § 11 BDSG und für Banken zudem aus § 25a Abs. 2 KWG zu beachten.

3.4 Bewertung der Implementierungsgüte

Die Güte eines IT GRC Managements ist vor allem davon abhängig, ob das hierzu durchgeführte **IT Risk Assessment** umfassend und zielgenau durchgeführt wurde. So sind auch an Stellen außerhalb der eigenen Stelle ausgelagerte Geschäftsprozesse und bestehende Outsourcing-Verhältnisse ausdrücklich beim IT Risk Assessment zu berücksichtigen. Dies wird leider in der Praxis viel zu oft vernachlässigt, weshalb die BaFin bei ihren aufsichtsrechtlichen Kontrollen bei Banken mittlerweile deutlich stärker darauf achtet, wie das umgesetzt ist. Auf der Ebene internationaler Standards hat das nunmehr ebenfalls Einzug gefunden in ISO/IEC 27036-3.

Ferner müssen die verwendeten Risikokataloge die tatsächlichen **Bedrohungen und Verwundbarkeiten** der zu betrachtenden Supporting Assets korrekt abbilden. In der Praxis werden dagegen oftmals Muster von Risikokatalogen bzw. Checklisten verwendet, die faktisch für die zu betrachtende Einrichtung unzutreffend bzw. ungenau sind. Die nötigen Anpassungen der eingesetzten Risikokataloge stellen daher die eigentliche Herausforderung bei der Gestaltung eines IT GRC Managements dar.

Auch ist in der Praxis immer wieder eine fehlende Verzahnung des IT-Risikomanagements mit dem **Corporate Risk Management** festzustellen. Das liegt vor allem daran, dass lediglich der monetäre Wert der eingesetzten IT-Komponenten anstelle der Werte der über die IT-Komponenten transportierten Informationen betrachtet wird, was somit zwangsläufig zu einer zu geringen Schadenshöhe führt.

Zudem gibt es bei IT-Risiken stärkere Ungenauigkeiten hinsichtlich der Bestimmung von **Eintrittswahrscheinlichkeiten**, als dies für andere Bereiche der Fall ist (siehe auch [Münch12], S. 327ff). Aufgrund der rasanten Fortentwicklung von IKT gibt es deutlich weniger tradierte Erfahrungswerte, wie sich ein IT-Risiko letztlich auswirkt, als dies für andere Bereiche gilt. Die Versuche, dies mittels Spieltheorie oder evidenzbasiert durch Einrichtung und Auswertung von Honey Nets / Pots zu schließen, konnte bislang diese Lücke noch nicht umfassend schließen. Zudem werden Banken teilweise mit gezielten Angriffen im Sinne von Advanced Persistent Threats (APT) konfrontiert.

Insofern wird zur Bewertung von IT-Risiken konsequenterweise eher auf eine **qualitative Betrachtung** zurückgegriffen, während alle anderen Risikoarten innerhalb einer Bank eher quantitativ betrachtet werden. Dies mit dem AMA-Ansatz zu vereinen, ist daher eine besondere Herausforderung für die Banken und erfordert, dass diese umfassende Datenbanken über eingetretene operationelle Risiken aufbauen. In Deutschland hat die zugehörige Diskussion hierzu aber erst begonnen.

4 Beispiele guter Praxis

Folgende Beispiele guter Praxis, an denen der Autor maßgeblich beteiligt war, dürften einen Eindruck vermitteln können, was für einen schlüssigen Aufbau eines IT GRC Managements nötig ist.

4.1 Harmonisierung einer internationalen Bankengruppe

Eine internationale Bankengruppe hat systematisch untersuchen lassen:

- Welche Anforderungen zur Informationssicherheit bestehen in den einzelnen Ländern, in denen Standorte der zur Gruppe gehörenden Banken betrieben werden?
- Welche Güte weisen die an diesen einzelnen Standorten bereits umgesetzten Organisationsrichtlinien zu Informationssicherheit und Business Continuity hinsichtlich dieser Anforderungen auf?
- Welcher Abdeckungsgrad wird in den einzelnen Standorten in Bezug auf beachtenswerte internationale Best Practice Standards zur Informationssicherheit und Business Continuity einerseits und hinsichtlich bestehender Gruppenvorgaben andererseits erreicht?
- Wie kann das bestehende Berichtswesen über Sicherheitsvorfälle harmonisiert werden, damit Sicherheitsvorfälle gruppenweit einheitlich dokumentiert werden, um aussagekräftige Werte im Sinne des AMA-Ansatzes liefern zu können?

Zielsetzung der in Auftrag gegebenen Analyse war es, bankgruppenweit ein einheitliches **Mindestniveau** an Informationssicherheit und Business Continuity zu erreichen, das alle bestehenden Anforderungen der Bankenaufsicht und internationaler Best Practice Standards abdeckt. Soweit die aufsichtsrechtlichen Anforderungen eines Landes höhere Anforderungen als die anderer Länder aufwiesen, war bankgruppenweit das höhere Niveau zu realisieren. Dabei wichen die aufsichtsrechtlichen Vorgaben teilweise grundlegend hinsichtlich Detaillierungsgrad und Umfang stark voneinander ab. Durch die vorgenommene Harmonisierung konnte das Gesamtniveau an Informationssicherheit und Resilienz in der Bankengruppe deutlich gesteigert werden. In diesem Zusammenhang wurden zahlreiche Synergieeffekte erzielt, zumal es bankengruppenintern zentrale Funktionen mit Wirkung auf die einzelnen Banken gab und füreinander zahlreiche Outsourcing-Services erbracht werden.

Alleine aufgrund der Größe der Bankengruppe und der Anzahl der zur Gruppe gehörenden Banken, samt deren jeweiligen Standorten, lieferten schließlich die dezentral nach einheitlichem Muster erfassten Angaben über festgestellte **Sicherheitsvorfälle** gruppenweit aussagekräftige Werte für statistische Auswertungen mit ausreichend hohen Fallzahlen. Die Bankengruppe tauschte darüber hinaus mit anderen Bankengruppen regelmäßig entsprechendes Datenmaterial aus, um eine bessere Abschätzung für Eintrittswahrscheinlichkeiten von Angriffen gewinnen zu können.

Im Rahmen des Projekts wurde zudem die zugehörige IT GRC Infrastruktur aufgebaut, um das erreichte Niveau dauerhaft halten zu können. Dieser Teil umfasste den Großteil des Projektvolumens. Die in diesem Beitrag aufgeführten Umsetzungsschritte wurden dabei erfolgreich in der Praxis angewandt. Ein nicht zu unterschätzender **Kollateraleffekt** des Projekts war, dass verschiedene Stellen innerhalb der Bankengruppe erstmals untereinander zu einem geregelten Informations- und Interessenaustausch gekommen sind und seither gemeinsam mit der Fortentwicklung der Informationssicherheit befasst sind.

4.2 Aufbau eines konsistenten Regelwerks

Eine große und bedeutsame international tätige Bank hat ihr bisheriges Regelwerk zur Informationssicherheit komplett überprüfen und grundlegend mit folgenden Zielsetzungen überarbeiten lassen:

- Das zu überarbeitende Regelwerk hat alle aktuellen rechtlichen und standardbezogenen Anforderungen zur Informationssicherheit wirksam zu adressieren.

- Das über die Zeit stark angewachsene Regelwerk an Organisationsrichtlinien ist zu harmonisieren und konsistent zu halten.
- Aus den überarbeiteten Regelwerksdokumenten sind Prüflisten zu generieren, die komfortable Rückmeldungen über die aktuelle Lage zur Informationssicherheit bei der Bank und Daten für entsprechende Metriken liefern.

Je komplexer eine Einrichtung und die zugehörige IKT sind, desto umfangreicher und komplexer ist letztlich das eingesetzte Regelwerk zur Informationssicherheit. Im Rahmen der durchgeführten Anpassungen konnten **systematische Regelungslücken** beseitigt werden. Die Bank hatte schon sehr frühzeitig damit angefangen, ein Regelwerk aufzubauen, in dem jedoch im Laufe der Zeit insbesondere infolge sich ändernder Zuständigkeiten wichtige Praxisfragen nicht mehr zielgenau zugewiesen wurden. Der formalisierte Anteil des Regelwerks wurde zwar gelebt, aber keine ganzheitliche Sichtweise vorgenommen. Die eingesetzte IKT wies eine sehr hohe Komplexität auf und viele automatisiert verarbeiteten Informationen hatten einen hohen Schutzbedarf.

Im Rahmen der durchgeführten Überarbeitungen wurde u.a. ein **passgenauer Risikokatalog** erstellt und das bisherige IT Risk Assessment effizienter und zielgenauer ausgerichtet. Neue Prozesse zur Gewährleistung von Informationssicherheit wurden eingerichtet und Zuständigkeiten klarer gefasst. Unnötige und zumeist zeitraubende Vorgehensweisen wurden konsequent eliminiert. Das Regelwerk wurde hierarchisch umstrukturiert und dabei die strategische Ebene (Leitlinie), taktische Ebene (Prozessbeschreibungen und Richtlinien) und operative Ebene (Maßnahmenpläne, Checklisten, Blaupausen, etc.) konsequent getrennt, wobei die höhere Ebene Zielvorgaben für die untere Ebene formuliert, die dort schließlich konkretisiert werden. Das unmittelbare Durchgreifen der oberen Regelwerksebene auf die ausführenden Regelwerksdokumente erhöhte die Transparenz über die Zusammenhänge und unterstrich nachvollziehbar die Bedeutung der Informationssicherheit. Auf diese Weise konnte schließlich eine optimale Steuerung der Informationssicherheit implementiert werden.

5 Ausblick

Ganzheitliche Informationssicherheit bei Banken ist ein umfangreiches Unterfangen, bei dem eine Vielzahl von Herausforderungen zu meistern ist. Die Praxis zeigt aber, dass in dem Fall, wenn diese Aufgaben nicht geschultert werden, eine höhere Anfälligkeit für Angriffe besteht. Dies lässt sich durch zahlreiche weitere durchgeführte Projekte belegen, an denen der Autor ebenfalls beteiligt war. Interessanterweise hatte sich u.a. gezeigt, dass im Laufe der Zeit attestierte Gefährdungen tatsächlich eingetreten sind, wenn entsprechende Empfehlungen (i.d.R. aufgrund des damit verbundenen Aufwands) ignoriert wurden. Die Auswirkungen, die entsprechend erfolgreiche Angriffe im Bankensektor haben können, können in solchen Fällen gravierend sein. Mit einem durchdachten IT GRC Management wird insoweit der Grad erreichter Informationssicherheit spürbar erhöht.

Literatur

[13569] ISO/TR 13569:2005 (Financial services – Information security guidelines)

[22301] ISO 22301:2012 (Societal security – Business continuity management systems – Requirements)

[22313] ISO 22313:2012 (Societal security – Business continuity management systems – Guidance)

[27000] ISO/IEC 27000:2012 (Information technology – Security techniques – Information security management systems – Overview and vocabulary)

[27001] ISO/IEC 27001:2013 (Information technology – Security techniques – Requirements)

[27002] ISO/IEC 27002:2013 (Information technology – Security techniques – Code of practice for information security management)

[27003] ISO/IEC 27003:2010 (Information technology – Security techniques – Information security management system implementation guidance)

[27005] ISO/IEC 27005:2011 (Information technology – Security techniques – Information security risk management)

[27013] ISO/IEC 27013:2012 (Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1)

[27014] ISO/IEC 27014:2013 (Information technology – Security techniques – Governance of information security)

[27015] ISO/IEC TR 27015:2012 (Information technology – Security techniques – Information security management guidelines for financial services)

[27031] ISO/IEC 27031:2011 (Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity)

[27035] ISO/IEC 27035:2011 (Information technology – Security techniques – Information security incident management)

[27036] ISO/IEC 27036-1:2014 (Information security for supplier relationships – Part 1: Overview and concepts) und ISO/IEC 27036-3:2013 (Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security); Teil 2 steht kurz vor der Veröffentlichung

[31000] ISO 31000:2009 (Risk management – Principles and guidelines)

[31004] ISO/TR 31004:2013 (Risk management – Guidance for the implementation of ISO 31000)

[AICPA11] American Institute of CPAs: Reporting on Controls at a Service Organization (SSAE No. 16)

[BFF12] Bundesanstalt für Finanzdienstleistungsaufsicht: MaRisk-Novelle 2012 - Veröffentlichung der Endfassung,
http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1210_anschreiben_ba.html (Abruf: 06.07.2014, 18:00 Uhr)

[BCBS10] Basel Committee on Banking Supervision: Principles for enhancing corporate governance
http://www.bis.org/publ/bcbs176.htm (Abruf: 06.07.2014, 18:00 Uhr)

[BCBS11] Basel Committee on Banking Supervision: Principles for the Sound Management of Operational Risk
http://www.bis.org/publ/bcbs195.pdf (Abruf: 06.07.2014, 18:00 Uhr)

[BCBS12] Basel Committee on Banking Supervision: Core principles for effective banking supervision
http://www.bis.org/publ/bcbs230.htm (Abruf: 06.07.2014, 18:00 Uhr)

[BCBS13] Basel Committee on Banking Supervision: Principles for effective risk data aggregation and risk reporting
http://www.bis.org/publ/bcbs239.pdf (Abruf: 06.07.2014, 18:00 Uhr)

[BCBS13] Basel Committee on Banking Supervision: International regulatory framework for banks (Basel III),
http://www.bis.org/bcbs/basel3.htm (Abruf: 06.07.2014, 18:00 Uhr)

[Brot09] Krag Brotby: Information Security Governance, Wiley (2009)

[BSI13] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, Stand: 13. Ergänzungslieferung
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html (Abruf: 06.07.2014, 18:00 Uhr)

[CaWa07] Alan Calder und Steve G. Watkins: Information Security Risk Management for ISO27001 / ISO17799, IT Governance Publishing (2007)

[COSO92] Committee of sponsoring Organizations of the Treadway Commission: Internal Control – Integrated Framework (COSO I, 1992)

[COSO04] Committee of sponsoring Organizations of the Treadway Commission: Enterprise Risk Management – Integrated Framework (COSO II, 2004)

[Eckh08] Jens Eckhardt: Rechtliche Grundlagen der IT-Sicherheit, DuD 5/2008, 330-336

[Heck06] Dirk Heckmann: Rechtspflichten zur Gewährleistung von IT-Sicherheit im Unternehmen, MMR 5/2006, 280-285

[HoMe10] Kevin Max von Holleben und Monika Menz: IT Risikomanagement – Pflichten der Geschäftsführung, CR 1/2010, 63-68

[IDW10] Institut der Wirtschaftsprüfer in Deutschland: Abschlussprüfung bei teilweiser Auslagerung der Rechnungslegung auf Dienstleistungsunternehmen (IDW PS 331)

[IDW13] Institut der Wirtschaftsprüfer in Deutschland: Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen (IDW PS 951 n.F.)

[IFA09] International Federation of Accountants: International Standard on Auditing 402 – Audit Considerations Relating to an Entity Using a Service Organization

[IFA11] International Federation of Accountants: International Standard on Assurance Engagements (ISAE) 3402 – Assurance Reports on Controls at a Service Organization

[ITGI12] IT Governance Institute: Control Objectives for Information and related Technology, Version 5

[Klip11] Sebastian Klipper: Information Security Risk Management, Vieweg+Teubner (2011)

[Köni13] Hans-Peter Königs: IT-Riskmanagement mit System, 4. Auflage, Springer Vieweg (2013)

[KSK11] Gerhard Klett, Klaus-Werner Schröder und Heinrich Kersten: IT-Notfallmanagement mit System, Vieweg+Teubner (2011)

[Lens07] Lars Lensdorf: IT-Compliance – Maßnahmen zur Reduzierung von Haftungsrisiken von IT-Verantwortlichen, CR 7/2007, 413-418

[Marb79] Peter Marburger: Die Regeln der Technik im Recht, Heymanns (1979)

[Münch12] Isabel Münch: Wege zur Risikobewertung. In: Peter Schartner & Jürgen Taeger (Hrsg): D-A-CH Security 2012, syssec (2012), 326-337

[OGC07] Office of Government Commerce: IT Infrastructure Library, Version 3

[Schm10] Michael Schmidl: Aspekte des Rechts der IT-Sicherheit, NJW 8/210, 476-481

[Seib13] Mark Seibel: Abgrenzung der „allgemein anerkannten Regeln der Technik“ vom „Stand der Technik“, NJW 41/2013, 3000-3004

[SoSo09] S.H. (Basie) von Solms und Rossouw von Solms: Information Security Governance, Springer (2009)

[Steg07] Udo Steger: Rechtliche Verpflichtung zur Notfallplanung im IT-Betrieb, CR 3/2007, 137-143

[StWi12] Artur Strasser und Michael Wittek: IT-Compliance, Informatik-Spektrum 1/2012, 39-44

[TeFe08] Alexander Teubner und Tom Feller: Informationstechnologie, Governance und Compliance, WI 5/2008, 400-407

[WiHe09] Bernhard C. Witt und Holger Heimann: Tool-Verbund für GRC und Sicherheit – Ansatz zur toolunterstützten Steuerung ganzheitlicher Informationssicherheit, <kes> 2009#2, 72-77

[Witt10] Bernhard C. Witt: IT Governance, Risk & Compliance Management – Praktische Erfahrungen. In: Michael Bartsch & Robert G. Briner (Hrsg): DGRI Jahrbuch 2010, Edition Informationstechnik und Recht, Schriftenreihe der Deutschen Gesellschaft für Recht und Informatik e.V., Band 20, Dr. Otto Schmidt (2010), 67-75

[Witt12] Bernhard C. Witt: Im Auftrag des Herrn – Theorie und Praxis der Auftragsdatenverarbeitung, <kes> 2012#2, 6-10