Legal Risk als Folge fehlender Compliance

Konzernrechtstag

Luther, Düsseldorf, 29.04.2015

Ludger Hanenberg – BaFin, Bonn.

Gliederung

1. Hintergründe
2. Compliance-Funktion als Risikomangement-Instrument
3. Befugnisse und Informationsrechte
4. Umfang rechtlicher Regelungen
5. Organisation der Compliance-Funktion

1. Rechtliche Grundlagen der Compliance-Funktion (1)

- Internationale Papiere und Vorgaben zur Compliance-Funktion bei Banken:
  - BCBS Core Principles (2012): Grundsatz 26 (Interne Kontrolle und Prüfung)

    → unabhängige interne Revisions- und Compliance-Funktionen zur Prüfung der Einhaltung einschlägiger Gesetze und Bestimmungen
  - BCBS „Compliance and the compliance function in banks" (April 2005)
  - BCBS „Principles for enhancing corporate governance" (Oktober 2010)
  - BCBS „Corporate governance principles for banks"

    → befinden sich in der Konsultationsphase (Ende: Januar 2015)
  - EBA „Guidelines on Internal Governance" (September 2011)

    → Guidelines lösen Kapitel 2.1 der CEBS „Guidelines on the application of the SRP under Pillar II" (Januar 2006) ab

1. Rechtliche Grundlagen der Compliance-Funktion (2)

- Nationale Vorgaben zur Compliance-Funktion bei Banken:
  - § 25a Abs. 1 Satz 1 KWG: „Ein Institut muss über eine ordnungsgemäße Geschäftsorganisation verfügen, die die Einhaltung der vom Institut zu beachtenden gesetzlichen Bestimmungen […]gewährleistet."

    → Einschub über das 4. FinanzmarktförderungsG (2002)
  - § 25a Abs. 1 Satz 3 Nr. 3c KWG:

    → Compliance-Funktion als expliziter Bestandteil des internen Kontrollsystems (und damit der laufenden Kontrollen in Abgrenzung zur IR als prozessunabhängige Kontrolle)

    → Konkretisierung in AT 4.4.2 der MaRisk
  - § 25c Abs. 4a Nr. 3c, Abs. 4b Nr. 3e KWG:=> Geschäftsleiter haben dafür Sorge zu tragen, dass das interne Kontrollsystem (der Gruppe) eine Compliance-Funktion umfasst

2. Compliance-Funktion als Risikomangement-Instrument (1)

- Grundsatz: Compliance-Funktion hat schwerpunktmäßig beratende und koordinierende Funktion → Unterstützung und Beratung der Geschäftsleitung in Compliance-relevanten Fragen
- Bestandsanalyse:
  - umfassende Analyse zur Identifizierung der wesentlichen rechtlichen Regelungen und Vorgaben (unter Compliance-Gesichtspunkten) → institutsindividuelle Orientierung am Geschäftsmodell vor dem Hintergrund der konkreten Geschäftsaktivitäten und der konkreten Märkte, auf denen das Institut tätig ist
- Aufbau- und Ablauforganisation:
  - (Hinwirken auf die) Implementierung wirksamer Verfahren zur Einhaltung (Compliance-relevanter) rechtlicher Regelungen und Vorgaben
  - Verhinderung von Umsetzungslücken insbesondere auch in Schnittstellenbereichen

2. Compliance-Funktion als Risikomangement-Instrument (2)

- Berichterstattung an die Geschäftsleitung → Weiterleitung an Aufsichtsorgan und IR
  - Regelmäßig, mindestens jährlich
  - Ad-hoc-Berichterstattung → Eskalation über die Geschäftsleitung bei Mängeln in den Verfahren zur Einhaltung gesetzlicher Regelungen und Vorgaben, schlagend werdender Compliance-Risiken etc.
  - Tätigkeitsbericht:
    - → Wirksamkeit der Verfahren ist darzustellen
    - → Angaben zu Defizite in den Verfahren und Kontrollen, die auf die Einhaltung rechtlicher Regelungen ausgerichtet sind
    - → Angaben zu möglichen Compliance-Risiken
    - → Angaben zu Maßnahmen zur Behebung der Defizite bzw. Risiken

2. Compliance-Funktion als Risikomangement-Instrument (3)

- Gesamtbericht über alle Compliance-Bereiche hinweg möglich; separate Berichte von WphG-Compliance und Geldwäscheprävention weiterhin möglich
- Integration auch Inhalte zu jenen Bereiche, auf die bei der Ausübung der Aufgaben zurückgegriffen wird, z.B. Risikocontrolling, Rechnungswesen

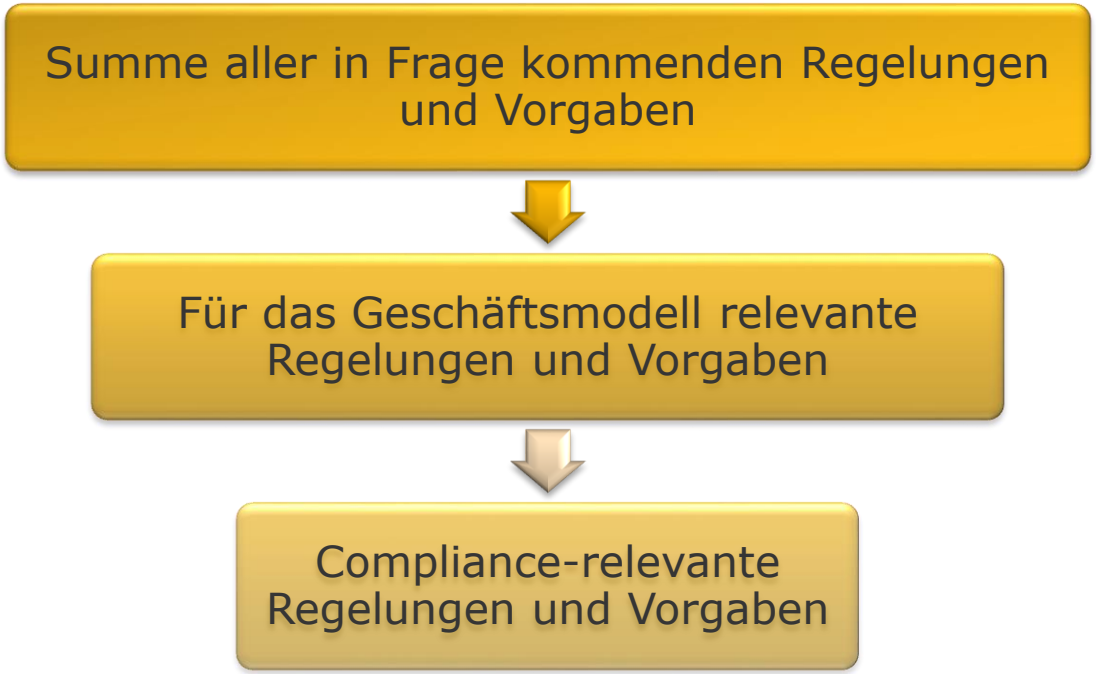
- Beteiligung an Anpassungsprozessen (AT 8 MaRisk):
  - Neu-Produkt-Prozess (AT 8.1 MaRisk)
  - Organisatorische Änderungen (AT 8.2 MaRisk)
  - IT-Systeme (AT 8.2 MaRisk)
- i.d.R. keine eigenen Prüfungshandlungen notwendig (unbeschadet möglicher Kontrollrechte => WphG-Compliance) aber: Kontrollhandlungen durch Compliance müssen möglich sein (entsprechende Kontrollrechte müssen vorhanden sein)

3. Umfang der rechtlichen Regelungen (1)

- Fokus der Compliance-Funktion sind wesentliche rechtliche Regelungen, deren Nichteinhaltung ein wesentliches Compliance-Risiko begründen, also zu einer Gefährdung des Vermögens des Instituts führen kann (vgl. AT 4.4.2, Tz. 1)
- Regelungsbereiche, die zwingend von der Compliance-Funktion zu adressieren sind:
  - Regelungen zu Wertpapierdienstleistungen
  - Regelungen zu Geldwäsche, Terrorismusfinanzierung
  - Regelungen zu sonstigen strafbaren Handlungen
  - Regelungen zum Verbraucherschutz (z.B. im Kreditgeschäft, Zahlungsverkehr)
  - Regelungen zum Datenschutz

3. Umfang der rechtlichen Regelungen (2)

- Identifizierung weiterer, unter Compliance-Gesichtspunkten wesentlicher Regelungen und Vorgaben durch die Compliance-Funktion (Wesentlichkeits- und Risikoanalyse)



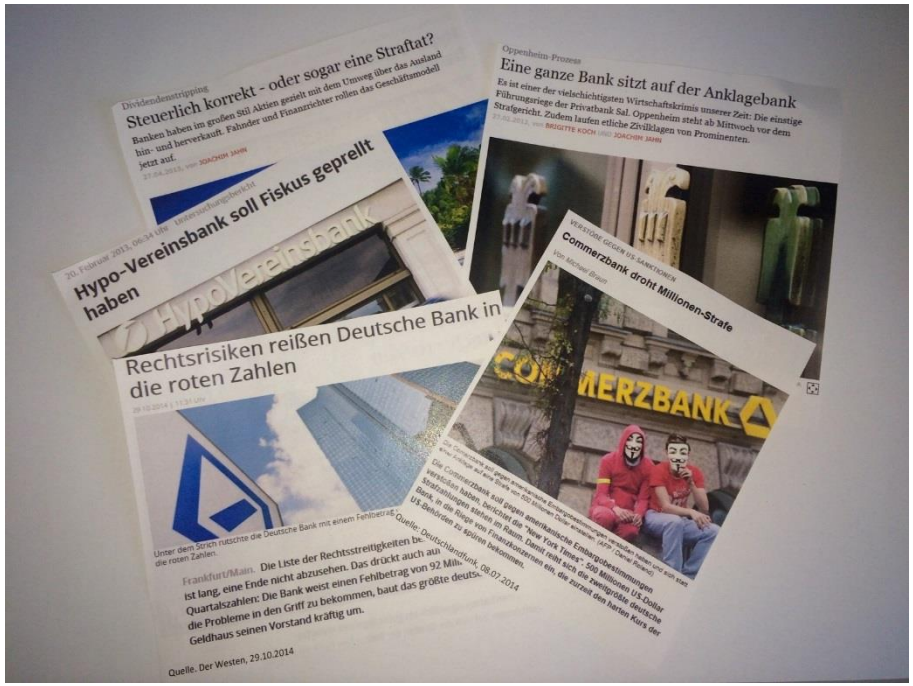
3. Umfang der rechtlichen Regelungen (3)

- Regelungsbereiche, die nicht zwingend von der Compliance-Funktion zu adressieren sind (**z. B.**):
  - Arbeitsrecht/Personalrecht
  - Einkommen-/Lohnsteuerrecht etc.
- **Sonderfälle**
  - Regelungen z.B. zu Risikotragfähigkeit, Risikocontrollingprozessen, Kapitalunterlegung (i.d.R. Verantwortlichkeit Risikocontrolling)
  - Bilanzrecht (Verantwortlichkeit Rechnungslegung/Finanzen)

  → Rückgriff auf spezialisiertes Wissen der zuständigen Einheiten möglich; (weitestgehende) Zurückstellung eigener Aktivitäten

4. Risiken bei fehlerhafter/fehlender Compliance (1)

- „If you think compliance is expensive, try non-compliance.“ (U.S. Deputy Attorney General Paul McNulty a.D.)



4. Risiken bei fehlerhafter/fehlender Compliance (2)

- Zielrichtung der Compliance-Funktion: Management der Compliance-Risiken
- Definition nach BCBS und EBA:

  → BCBS: Risiko rechtlicher oder aufsichtlicher Sanktionen, materieller finanzieller Verluste, oder eines Reputationsverlustes aufgrund der Nichtbeachtung von Gesetzen, Verordnungen, Regelungen, Industriestandards und Verhaltenskodizes

  → EBA: aktuelles oder zukünftiges Risiko für Erträge und Kapital aufgrund von Verstößen und Nichtbeachtung von Gesetzen, Verordnungen, vorgeschriebener Geschäftspraktiken und ethischen Standards

4. Risiken bei fehlerhafter/fehlender Compliance (3)

- MaRisk verzichten auf den Begriff „Compliance-Risiken“; vielmehr Umschreibung der Risiken: „Risiken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben ergeben können (AT 4.4.2, Tz. 1)“
- Risiken, die sich als Compliance-Risiken realisieren können:
  - Rechtsrisiken
  - operationelle Risiken
  - Reputationsrisiken

Glossar

- BCBS: Baseler Ausschuss für Bankenaufsicht (Basel Committee on Banking Supervision)
- CEBS: Ausschuss der Europäischen Aufsichtsbehörden für das Bankwesen (Committee of European Banking Supervisors) → mit Wirkung zum 1. Januar 2011 in der EBA aufgegangen
- EBA: Europäische Bankenaufsichtsbehörde (European Banking Authority)
- MaRisk: Mindestanforderungen an das Risikomanagement, Rundeschreiben der BaFin 10/2012

BaFin

Vielen Dank für Ihre Aufmerksamkeit!

Ludger Hanenberg

Tel. +49 (0)228 / 41 08-1582
ludger.hanenberg@bafin.de