

Gesamtverantwortung der Geschäftsleitung (auch für angemessene Risikokultur) (AT 3)

Risikomanagement (AT 4)

auch auf Gruppenebene (AT 4.5)

Risikotragfähigkeit (AT 4.1)

Gesamtrisikoprofil

auf Basis einer Risikoinventur unter Berücksichtigung von Risikokonzentrationen und validierten Diversifikationseffekten

- Berücksichtigung der wesentlichen Risiken
- Begründungspflicht bei Nutzung der Ausnahmemöglichkeit
- Überprüfung der eingesetzten Methoden und Verfahren, ggf. unter Funktionstrennung von Entwicklung und Validierung

Methoden- und Verfahrensfreiheit für die Beurteilung, angemessene Berücksichtigung von Going-Concern- und Liquidationsaspekten

Begründung der zugrunde liegenden Annahmen sowie Genehmigung wesentlicher Elemente durch die Geschäftsleitung

Risikodeckungspotenzial

- Laufende Abdeckung der wesentlichen Risiken
- Individuelle Definition

Zukunftsgerichteter Kapitalplanungsprozess



Geschäftsstrategie (AT 4.2)

Risikostrategie (AT 4.2)

Ressourcen (AT 7)

Personal (AT 7.1)

- Quantitative und qualitative Anforderungen mit besonderen Anforderungen für die Leitung der in AT 4.4 genannten Funktionen
- Vertretungsregelung

Technisch-organisatorische Ausstattung (AT 7.2)

- Sicherstellung der Integrität, Verfügbarkeit, Authentizität und Vertraulichkeit der Daten
- Abstellen auf gängige Standards
- Implementierung von Regelprozessen zu Test und Abnahme
- Entsprechende Beachtung beim Einsatz von IDV unter Beachtung des jeweiligen Schutzbedarfs

Notfallkonzept (AT 7.3)

- Geschäftsfortführungs- und Wiederanlaufpläne
- Regelmäßige Notfalltests und Berichterstattung
- Festlegung der Kommunikationswege

Interne Revision (AT 4.4.3, BT 2)

- Aufgaben und Grundsätze (AT 4.4.3, BT 2.1, BT 2.2)
- Prüfungsplanung und -durchführung (AT 4.4.3, BT 2.3)
- Berichtspflicht (AT 4.4.3, BT 2.4)
- Reaktion auf festgestellte Mängel (AT 4.4.3, BT 2.5)

Interne Kontrollverfahren

Internes Kontrollsystem (AT 4.3, BT 1)

Aufbau- und Ablauforganisation (AT 4.3.1)

- Grundsätzliche Funktionstrennung inkl. Cooling-Off-Perioden bei Wechsel von Markt-/Handelsbereichen in Kontrollbereiche
- Klare Definition und Abstimmung aller Prozesse
- Regelmäßige und anlassbezogene Überprüfung von IT- und Zeichnungsberechtigungen sowie Kompetenzen

Aufbau- und Ablauforganisation im Kredit- und Handelsgeschäft (BTO)

Kreditgeschäft (BTO 1)

- Besondere Funktionstrennung und Votierung (BTO 1.1)
- Kreditprozesse (BTO 1.2)
- Risikofrüherkennung (BTO 1.3)
- Risikoklassifizierung (BTO 1.4)

Handelsgeschäft (BTO 2)

- Besondere Funktionstrennung und Votierung (BTO 1.1)
- Kreditprozesse (BTO 1.2)
- Risikofrüherkennung (BTO 1.3)
- Risikoklassifizierung (BTO 1.4)

Risikosteuerungs- und -controllingprozesse (AT 4.3.2, BTR)

Identifizierung, Beurteilung, Steuerung, Überwachung sowie Kommunikation von

- Adressenausfallrisiken (BTR 1)
  - Marktpreisrisiken (BTR 2, BTR 2.1)
    - Marktpreisrisiken des Handelsbuches (BTR 2.2)
    - Marktpreisrisiken des Anlagebuches (BTR 2.3)
  - Liquiditätsrisiken (BTR 3, BTR 3.1)
    - Zusätzliche Anforderungen an kapitalmarktorientierte Institute (BTR 3.2)
  - Operationellen Risiken (BTR 4)
    - unter Berücksichtigung von Risikokonzentrationen und Stresstestergebnissen im Rahmen einer Gesamtbanksteuerung sowie wirksame Begrenzung unter Berücksichtigung der Risikotragfähigkeit und des Risikoappetits.
- Auch für IT-Risiken sind angemessene Risikosteuerungs- und -controllingprozesse einzurichten.

Stresstests (AT 4.3.3)

- Unterschiedliche Szenarien inkl. schwerer Downside-Szenarien, Stresstests für das Gesamtrisikoprofil und inverser Stresstests
- Kritische Reflexion der Ergebnisse

Datenmanagement, Datenqualität und Aggregation von Risikodaten (AT 4.3.4)

- gilt nur für große & komplexe Institute/Gruppen
- Festlegung von entsprechenden Grundsätzen durch die Geschäftsleitung
- Risikodaten müssen genau, vollständig sowie nach verschiedenen Kategorien auswertbar sein, plausibilisiert werden und auch in Stressphasen zeitnah verfügbar sein
- Hinreichende Flexibilität und Leistungsfähigkeit von Datenaggregationskapazitäten
- Festlegung von Verantwortlichkeiten, prozessabhängigen Kontrollen sowie Überprüfung durch unabhängige Stelle

Risikocontrolling-Funktion (AT 4.4.1)

- Unabhängige Funktion für Risiko-Überwachung und -Kommunikation
- uneingeschränktes und jederzeitiges Informationsrecht
- Ausreichend hohe Führungsebene, bei großen & komplexen Instituten CRO (≠ CFO oder COO)

Compliance-Funktion (AT 4.4.2)

- Implementierung wirksamer Compliance-Verfahren & Kontrollen
- Bei großen & komplexen Instituten eigenständige Organisationseinheit unmittelbar unterhalb der Geschäftsleiterebene

Anforderungen an die Risikoberichterstattung (BT 3)

- Nachvollziehbarkeit & Aussagefähigkeit inkl. Beurteilung der Risikosituation und zukunftsorientierter Risikoeinschätzung
- turnusmäßig & ad hoc
- Erstellung in zeitlich angemessenem Rahmen
- Vierteljährliche Information des Aufsichtsorgans
- Besondere Anforderungen für die Berichterstattung der Risikocontrolling-Funktion, der Compliance-Funktion, der Markt- und Handelsbereiche sowie zu Auslagerungen

Dokumentation (AT 6)

Organisationsrichtlinien (AT 5)

Anpassungsprozesse (AT 8)

Auslagerung (AT 9)