

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, in komplexen Fällen unter angemessener Unabhängigkeit von Entwicklung und Validierung

Methoden- und Verfahrensfreiheit für die Beurteilung, angemessene Berücksichtigung von normativer und ökonomischer Perspektive

Begründung der zugrundeliegenden Annahmen sowie Genehmigung wesentlicher Elemente durch die Geschäftsleitung

Risikodeckungspotenzial

- Laufende Abdeckung der wesentlichen Risiken
- Individuelle Definition

Zukunftsgerichteter Kapitalplanungsprozess



Ressourcen (AT 7)

Personal (AT 7.1)

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

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
- Einrichtung angemessener Überwachungs- und Steuerungsprozesse für IT-Risiken
- Entsprechende Beachtung beim Einsatz von IDV
- Konkretisierung durch die BAIT

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)

Geschäftsstrategie (AT 4.2)

Risikostrategie inkl. Risikoappetit (AT 4.2)

Interne Kontrollverfahren

Internes Kontrollsystem (AT 4.3, BT 1)

Aufbau- und Ablauforganisation (AT 4.3.1, BTO)

- Grundsätzliche Funktionstrennung inkl. Cooling-Off-Perioden bei Wechsel von Handels-/Marktbereichen in Kontrollbereiche
- Klare Definition und Abstimmung aller Prozesse
- Need-to-Know-Prinzip für Berechtigungen und Kompetenzen
- Regelmäßige und anlassbezogene Überprüfung von IT- und Zeichnungsberechtigungen sowie Kompetenzen

Kreditgeschäft (BTO 1)

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

Handelsgeschäft (BTO 2)

- Besondere Funktionstrennung (BTO 2.1)
- Handelsprozesse (BTO 2.2)
  - Handel
  - Abwicklung und Kontrolle
  - Risikocontrolling

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)
  - Allgemeine Anforderungen inkl. Erstellung eines internen Refinanzierungsplans (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

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 für systemrelevante Institute/Gruppen
- Festlegung von entsprechenden Grundsätzen durch die Geschäftsleitung
- Sicherstellung der Integrität, Auswertbarkeit und zeitnahen Verfügbarkeit von Risikodaten, auch in Stressphasen
- Hinreichende Flexibilität 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 systemrelevanten Instituten CRO (≠ CFO oder COO)

Compliance-Funktion (AT 4.4.2)

- Implementierung wirksamer Compliance-Verfahren & Kontrollen
- Unmittelbar der Geschäftsleitung unterstellt bzw. direkte Berichtslinie, bei systemrelevanten Instituten eigenständige Organisationseinheit

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 über die Risikosituation
- Besondere Anforderungen für die Berichte der Risikocontrolling-Funktion

Dokumentation (AT 6)

Organisationsrichtlinien (AT 5)

Anpassungsprozesse (AT 8)

Auslagerung inkl. zentrales Auslagerungsmanagement (AT 9)