

THALVENIA BANK AG

Compliance-Handbuch — Auszug

Kapitel 2: AML/GwG | Kapitel 3: IT-Sicherheit/BAIT

Version 3.3 | Stand: Oktober 2025 | Vertraulich — Nur fuer interne Verwendung

Kapitel 2: AML-Organisation und GwG-Pflichten

2.1 Geldwaeschebeauftragter (§ 7 GwG)

Geldwaeschebeauftragter i.S.d. § 7 Abs. 1 GwG ist der Chief Compliance Officer (CCO). Er ist dem Vorstand unmittelbar unterstellt und in seiner Meldefunktion weisungsunabhaengig. Stellvertreter ist die AML-Analystin. Der Geldwaeschebeauftragte ist der alleinige Ansprechpartner fuer Verdachtsmeldungen nach § 43 GwG an die FIU.

2.2 Kundensorgfaltspflichten (§§ 10-15 GwG)

Alle Neukunden sind bei Beginn der Geschaeftsbeziehung zu identifizieren. Hochrisikokunden (Kategorie 3 und 4) unterliegen den verstaerkten Sorgfaltspflichten nach § 15 GwG. Die PEP-Pruefung erfolgt mittels SymphonyAI Sensa (Tier 1 + Tier 2 seit April 2026). Die Risikoklassifizierung ist bei Hochrisikokunden jaehrlich zu aktualisieren; bei Standardkunden alle zwei Jahre.

2.3 Verdachtsmeldepflicht (§ 43 GwG)

Bei Hinweisen auf Geldwaesche oder Terrorismusfinanzierung ist ohne schuldhaftes Zoegern eine Verdachtsmeldung (STR) an die FIU ueber das goAML-Portal zu erstatten. Jede interne Analyse — auch wenn keine Meldung erfolgt — ist vollstaendig zu dokumentieren. Das Tipping-off-Verbot nach § 44 GwG ist strikt einzuhalten.

2.4 Transaktionsmonitoring

Das Transaktionsmonitoring-System (Chainalysis Reactor) erzeugt automatische Flags bei Auffaelligkeiten. Jeder Flag ist innerhalb von 2 Werktagen durch den AML-Analysten zu beurteilen. Bei Risikoscore > 7 ist der Geldwaeschebeauftragte zu informieren. Das Regelwerk ist jaehrlich zu aktualisieren.

Kapitel 3: IT-Sicherheit (BAIT 2024)

3.1 Anzeigepflicht IT-Sicherheitsvorfaelle (BAIT Tz. 55)

Wesentliche IT-Sicherheitsvorfaelle sind der BaFin unverzueglich zu melden, spaetestens innerhalb von 24 Stunden nach Kenntniserlangung. Als 'wesentlich' gilt ein Vorfall, wenn

Vertraulichkeit, Integrität oder Verfügbarkeit von Kundenvermögenswerten oder kritischen Systemen beeinträchtigt ist. Ab IT-Notfall Stufe 2 ist der CISO zur sofortigen BaFin-Meldung verpflichtet, unabhängig vom Informationsstand. Folgemeldungen sind bei neuen Erkenntnissen zu erstatten.

3.2 Schwachstellenmanagement

Kritische Schwachstellen (CVSS-Score > 9.0) sind innerhalb von 72 Stunden nach CVE-Veröffentlichung zu patchen. Alle anderen Schwachstellen (CVSS > 7.0) sind innerhalb von 14 Tagen zu beheben. Der CISO führt ein vollständiges Schwachstellen-Register. Ungepatchte Systeme sind dem Vorstand monatlich zu melden.

3.3 Business Continuity Management

Für alle kritischen Systeme (MPC-Signing, Cold Custody, Core Banking) sind Disaster-Recovery-Pläne (Notfallkonzept Stand Juli 2026) vorhanden. DR-Tests erfolgen halbjährlich. Recovery Time Objective (RTO): 4 Stunden für Kritisch-1-Systeme. Recovery Point Objective (RPO): 1 Stunde.

Quellen:

[1] GwG §§ 4-12, 43, 44: [gesetze-im-internet.de/gwg](https://www.gesetze-im-internet.de/gwg) | [2] MaRisk BA 2024: [bafin.de/MaRisk-2024](https://www.bafin.de/MaRisk-2024) | [3] BAIT 2024: [bafin.de/BAIT](https://www.bafin.de/BAIT) | [4] MiCAR Art. 89-92: [EUR-Lex MiCAR](https://eur-lex.europa.eu/lexicon/micar)