

Arbeitsakte

Akte: BaFin-Sonderprüfung Thalvenia Bank AG — Kryptoverwahrung, AML-Pflichtverletzungen, MiCAR-Lizenzkrise

bafin-verfahren-kryptoverwahrung-thalvenia-bank-aufsichtsverletzung-stuttgart

Die ZIP-URL ist stabil und zeigt immer auf die aktuelle Version. Im Akten-ZIP ist das Gesamt-PDF mit enthalten.

Diese Datei bündelt alle Aktenstücke in einem Dokument. Die Einzeldateien liegen im Aktenordner ebenfalls vor.

Inhaltsverzeichnis

Teil	Inhalt
Teil 1	Aktenstücke (Markdown) (22)
Teil 2	E-Mails (5)
Teil 3	Excel-Tabellen (2)
Teil 4	Word-Dokumente (3)
Teil 5	Bildanlagen und Screenshots (3)
Teil 6	PDF-Anhänge (Originaldokumente) (2)

Aktenstücke (Markdown)

Datei: 01-mandatsuebernahme-thalvenia.md

01 — Mandatsübernahme Thalvenia Bank AG

Kanzlei: Schwertbeck Roosendaal mbB, Frankfurt am Main

Federführung: Prof. Dr. Heinrich Schwertbeck

Aktenzeichen Kanzlei: SR-2026-FIN-0612

Datum Mandatserteilung: 20. März 2026

Mandantin: Thalvenia Bank AG, Königstraße 87, 70173 Stuttgart

Sachverhalt bei Mandatserteilung

Am 18. März 2026 ging bei der Kanzlei Schwertbeck Roosendaal ein dringender Anruf von CEO Dr. Cornelius Thalheim-Lattermann und CCO Dr. Lasse Tannenfels ein. Hintergrund war die am selben Tag zugegangene Prüfungsmitteilung der BaFin (Az. VBS 4 1 7-K-22-188/2026), mit der eine Sonderprüfung nach § 44 KWG mit sofortiger Wirkung eingeleitet wurde. Das Institut hatte zu diesem Zeitpunkt keinen spezialisierten Bankaufsichtsrechtler mandatiert; die bisherige Hausanwaltskanzlei war ausschließlich im Bereich Gesellschaftsrecht tätig.

Prof. Dr. Schwertbeck war am 19. März 2026 zu einem Vorgespräch in Stuttgart. Anwesend waren alle vier Vorstandsmitglieder sowie die interne Leiterin der Rechtsabteilung, Dr. Miriam Hoffrath-Seel. Das Gespräch dauerte rd. vier Stunden.

Konfliktprüfung und Interessenlage

Vor Mandatserteilung war zu prüfen, ob die Vertretung aller Vorstandsmitglieder durch dieselbe Kanzlei möglich ist. Folgende Risikokonstellationen wurden erörtert:

1. **CCO Dr. Tannenfels:** Staatsanwaltschaft Stuttgart führt seit Februar 2026 ein Ermittlungsverfahren wegen des Verdachts der Geldwäsche (§ 261 StGB, Az. 13 Js 4481/26). Eine Interessenkollision zwischen Individualverteidigung und Institutsvertretung ist möglich.
2. **CRO Dr. Birkenhainer:** Keine bekannten Individualverfahren; Vertretung durch Schwertbeck Roosendaal unbedenklich.
3. **CEO und COO:** Keine Individualverfahren; Vertretung unbedenklich.

Ergebnis Konfliktprüfung: Schwertbeck Roosendaal übernimmt das Mandat für die Thalvenia Bank AG als Institut sowie für CEO, COO und CRO in ihrer Eigenschaft als Vorstandsmitglieder. Für CCO Dr. Tannenfels wird eine **getrennte Strafverteidigung** empfohlen; RAin Dr. Franziska Oberkampf-Heyden, Frankfurt, wird als Strafverteidigerin mandatiert. Schwertbeck Roosendaal koordiniert mit ihr soweit keine Interessenkollision besteht.

Vollmacht

Vollmacht erteilt durch Vorstandsbeschluss der Thalvenia Bank AG vom 20. März 2026 (einstimmig, CCO enthielt sich wegen Individualinteressen). Die Vollmacht umfasst:

- Vertretung gegenüber der BaFin im Sonderprüfungsverfahren VBS 4 1 7-K-22-188/2026
- Vertretung gegenüber der FIU im Verfahren 2026-FIU-7711-TN
- Beratung im MiCAR-Zulassungsverfahren
- Koordination mit Staatsanwaltschaft Stuttgart (soweit institutsseitig)
- Presserechtliche Begleitung

Retainer und Honorar

Vereinbart: Stundenhonorar Prof. Dr. Schwertbeck EUR 650/Stunde zzgl. MwSt.; Dr. Glock-Meinhard EUR 420/Stunde; RA Freytag-Sonnleitner EUR 380/Stunde. Monatlicher Kostenvorschuss EUR 75.000 für die ersten drei Monate. Anzahlung EUR 150.000 bei Mandatserteilung. Kein Erfolgshonorar.

Sofortmaßnahmen (20./21. März 2026)

1. **Aktensicherung:** Interne Anweisung an alle Abteilungen, keine Dokumente zu löschen oder zu verändern (Legal Hold).
2. **Kommunikationskontrolle:** Alle externen Kommunikationen mit BaFin, FIU und Staatsanwaltschaft laufen ab sofort über die Kanzlei.
3. **Prüferkontakt:** Kanzlei nimmt Kontakt mit der leitenden Prüferin Dr. Hannelore Kösters (BaFin, Referat VBS 4) auf.
4. **Datenraum:** Einrichtung eines verschlüsselten Datenraums (iManage) für Dokumentenübergabe an Prüfer.
5. **Krisenteam:** Konstituierung eines internen Krisenteams bestehend aus CCO, CRO, Leiterin Rechtsabteilung und externem Berater (Schwertbeck Roosendaal).

Offene Fragen bei Mandatsübernahme

- Umfang der AML-Lücken (interne Aufarbeitung noch nicht abgeschlossen)
- Genaue Tatbestandsmerkmale des Cybervorfall-Meldungsversäumnisses (Fristberechnung BAIT Tz. 55)
- Stand des MiCAR-CASP-Antrags und Vollständigkeit der Unterlagen
- Ob BaFin bereits eine Untersagungsverfügung nach § 6 KWG vorbereitet
- Verbindlichkeit der FIU-Anfrage und Umfang der Auskunftspflicht

Bearbeiterin: Prof. Dr. Heinrich Schwertbeck / Dr. Petra Glock-Meinhard

Nächste Schritte: Vgl. 04-bafin-pruefungsmitteilung-2026.md,
05-pruefungsschwerpunkte-aml-cybersecurity.md

Datei: 02-historische-kryptoverwahrungslizenz-2020.md

02 — Historische Kryptoverwahrungslizenz 2020

Datum Zulassung: 15. Oktober 2020

Aktenzeichen BaFin (historisch): VBS 4 1 2-K-24-0118/2020

Zugelassenes Geschäft: Kryptoverwahrungsgeschäft gem. § 1 Abs. 1a S. 2 Nr. 6 KWG (in der ab 01.01.2020 gültigen Fassung)

Gesellschaftsstruktur

Die Thalvenia Bank AG wurde im Jahr 2018 als Thalvenia GmbH gegründet und im Jahr 2019 in eine Aktiengesellschaft nach deutschem Recht umgewandelt. Sitz ist Stuttgart. Die Gesellschaft ist eingetragen im Handelsregister des Amtsgerichts Stuttgart unter HRB 76442.

Aktionärsstruktur (Stand März 2026):

Aktionär	Anteil
Thalheim-Lattermann Familienstiftung, Liechtenstein	41,2 %
Vellbruck Capital GmbH, Frankfurt	18,7 %
Streubesitz (institutionelle Investoren)	31,4 %
Eigene Aktien	8,7 %

Kein Aktionär hält eine qualifizierte Beteiligung i.S.d. § 2c KWG, die eine gesonderte Inhaberkontrolle ausgelöst hätte, mit Ausnahme der Thalheim-Lattermann Familienstiftung, deren Beteiligung von der BaFin 2019 geprüft und genehmigt wurde.

Geschäftsmodell bei Zulassung 2020

Das Institut beantragte 2019 die Zulassung zum Betreiben des Kryptoverwahrungsgeschäfts i.S.d. § 1 Abs. 1a S. 2 Nr. 6 KWG, das durch das Gesetz zur Umsetzung der Änderungsrichtlinie zur vierten EU-Geldwäscherichtlinie (BGBl. I 2019, S. 2602) mit Wirkung zum 01.01.2020 in das KWG aufgenommen worden war.

Gegenstand des Kryptoverwahrungsgeschäfts ist die Verwahrung, Verwaltung und Sicherung von Kryptowerten oder privaten kryptografischen Schlüsseln, die dazu dienen, Kryptowerte zu halten, zu speichern oder zu übertragen, für andere (§ 1 Abs. 1a S. 2 Nr. 6 KWG).

Das Institut bot bei Zulassung drei Kerndienste an:

1. **Cold-Custody-Dienst** für institutionelle Anleger (Verwaltung privater Schlüssel in HSM-gesicherter Offline-Umgebung)
2. **Multi-Party-Computation (MPC) Signing Service** für qualifizierte Anleger
3. **Staking-as-a-Service** (ab 2022 hinzugekommen, nachträglich von BaFin toleriert)

Bilanzvolumen bei Zulassung: Verwaltetes Kundenvermögen rd. EUR 180 Mio.

Verwaltetes Kundenvermögen März 2026: EUR 4,3 Mrd. (Wachstum durch Institutionalisierung des Kryptomarkts)

Auflagen bei Zulassung 2020

Die BaFin erteilte die Zulassung unter folgenden Nebenbestimmungen:

1. Vorlage eines geprüften IT-Sicherheitskonzepts nach BAIT innerhalb von sechs Monaten.
2. Benennung eines hauptamtlichen Compliance-Officers (CCO) mit ausgewiesener AML-Expertise innerhalb von drei Monaten.
3. Abschluss einer Betriebshaftpflichtversicherung mit Mindestdeckung EUR 10 Mio. pro Schadensfall.
4. Jährliche Vorlage eines externen IT-Prüfberichts (SOC 2 Type II oder gleichwertig).

Auflagenerfüllung: Nach interner Auskunft der Rechtsabteilung wurden die Auflagen 1-3 fristgerecht erfüllt. Auflage 4 (IT-Prüfbericht) wurde für die Prüffahre 2020-2023 erfüllt; der Bericht für 2024 lag bei Einleitung der Sonderprüfung noch nicht vor — dies ist einer der Anknüpfungspunkte der BaFin-Prüfung.

Personelle Besetzung des Vorstands

Dr. Cornelius Thalheim-Lattermann (CEO) ist seit Gründung dabei; er war bereits Geschäftsführer der Thalvenia GmbH. Marc Vellbruck (COO) stieß 2021 hinzu. Dr. Annegret Birkenhainer (CRO) wurde 2022 bestellt. Dr. Lasse Tannenfels (CCO) wurde im Oktober 2020, unmittelbar nach Zulassung, bestellt — er war zuvor AML-Officer bei einer Regionalbank.

Die BaFin prüfte die Zuverlässigkeit und fachliche Eignung aller Vorstandsmitglieder nach § 33 Abs. 1 KWG; alle Prüfungen verliefen ohne Beanstandung.

Relevanz für die Sonderprüfung 2026

Die historische Zulassung ist für das aktuelle Verfahren in mehrfacher Hinsicht relevant:

- Die Auflagenlücke beim IT-Prüfbericht 2024 gibt der BaFin einen formalen Ansatzpunkt.
- Das Wachstum des verwalteten Kundenvermögens von EUR 180 Mio. auf EUR 4,3 Mrd. hat die Risikoprofile der Kunden grundlegend verändert, ohne dass die AML-Systeme proportional skaliert wurden.
- Die ursprünglichen Kundenidentifikationsverfahren stammten aus 2020 und wurden trotz Überarbeitung des GwG und BaFin-Auslegungshinweisen nicht durchgehend aktualisiert.

Vgl. hierzu 07-aml-pflichten-gwg-katalog.md und 08-kundenidentifikation-kyc-mangel.md.

Datei: 03-mica-vermoegensanlagengesetz-uebergang.md

03 — MiCAR-Übergangslizenz und Übergangsregime

Rechtsgrundlage: Verordnung (EU) 2023/1114 über Märkte für Kryptowerte (MiCAR), insb. Art. 59, Art. 63, Art. 143

Nationales Umsetzungsgesetz: Finanzmarktdigitalisierungsgesetz (FinmadiG), BGBl. I 2024

Antragsdatum CASP-Zulassung: 14. November 2024

Zuständige Behörde: BaFin (Referat WA 37)

Übergangsregime nach Art. 143 MiCAR

Art. 143 Abs. 3 MiCAR sieht vor, dass Unternehmen, die vor dem 30. Dezember 2024 nach nationalem Recht zugelassen waren und Kryptoasset-Dienstleistungen erbringen, diese Dienstleistungen bis zum 1. Juli 2026 (oder bis zur nationalen Verkürzung auf 12 Monate) ohne CASP-Zulassung nach MiCAR fortführen dürfen. Der deutsche Gesetzgeber hat im FinmadiG die Übergangsfrist auf den 30. Juni 2026 begrenzt.

Die Thalvenia Bank AG befindet sich somit im Übergangsregime. Der CASP-Antrag vom 14. November 2024 wurde vollständig eingereicht; die BaFin hat die Vollständigkeit am 20. Januar 2025 bestätigt. Die Prüfung dauert an; eine Entscheidung wurde für das zweite Quartal 2026 in Aussicht gestellt.

Antragsinhalt (Zusammenfassung)

Der CASP-Antrag umfasst die Zulassung für folgende Kryptoasset-Dienstleistungen nach Art. 3 Abs. 1 Nr. 16 MiCAR:

MiCAR-Dienstleistung	Art. MiCAR	Status Antrag
Verwahrung und Verwaltung von Kryptowerten für Kunden	Art. 3 Abs. 1 Nr. 16 lit. a	Beantragt
Betrieb einer Handelsplattform für Kryptowerte	Art. 3 Abs. 1 Nr. 16 lit. b	Beantragt (neu)
Ausführung von Aufträgen für Kryptowerte	Art. 3 Abs. 1 Nr. 16 lit. d	Beantragt (neu)
Entgegennahme und Übertragung von Aufträgen	Art. 3 Abs. 1 Nr. 16 lit. e	Beantragt (neu)

Die Erweiterung auf Dienstleistungen b, d und e ist für das Institut strategisch bedeutsam und erklärt teilweise das Wachstum des Kundenvolumens im Jahr 2024. Diese Erweiterung ist jedoch kritisch zu sehen, weil das operative Ausrollen dieser neuen Dienste im Jahr 2024 unter dem Übergangstatus erfolgte und die AML-Systeme nicht zeitgerecht angepasst wurden.

Aufsichtsrechtliche Anforderungen unter MiCAR

Im Gegensatz zum früheren KWG-Regime stellt MiCAR deutlich erhöhte Anforderungen:

- **Kapitalanforderungen** nach Art. 67 MiCAR: Mindestkapital EUR 150.000 (derzeit EUR 12,5 Mio. Eigenkapital, gut erfüllt).
- **Governance** nach Art. 68 MiCAR: Mindestens zwei Leitungsmitglieder erforderlich — erfüllt.
- **White Paper** für jede angebotene Kryptowertart nach Art. 6 ff. MiCAR — ausstehend für drei neue Token-Kategorien.
- **Regeln über Interessenkonflikte** nach Art. 72 MiCAR — Lücken identifiziert im Zusammenhang mit dem Eigenhandel Token TN.

- **AML-/CFT-Anforderungen** nach Art. 92 MiCAR i.V.m. AMLA — entsprechen weitgehend dem GwG, verschärft durch Transfer of Funds Regulation (TFR).

Gefährdung der Übergangslizenz

Die BaFin hat im Anhörungsschreiben vom 14. Juli 2026 ausdrücklich darauf hingewiesen, dass die festgestellten Mängel (AML, Cyber, MAR) bei einer Gesamtbewertung die Versagung der CASP-Zulassung nach Art. 63 Abs. 1 lit. b MiCAR rechtfertigen können, wenn das Institut nicht zuverlässige und solide Regelungen und Verfahren zur Prävention von Geldwäsche und Terrorismusfinanzierung vorhält. Zusätzlich droht nach § 6 Abs. 3 KWG eine Untersagung der Kryptoverwahrgeschäfte bereits vor Ablauf der Übergangsfrist, wenn der ordnungsgemäße Geschäftsbetrieb gefährdet erscheint.

Zeitdruck: Die Übergangsfrist endet am 30. Juni 2026. Der aktuelle Stand (August 2026) bedeutet, dass das Institut bereits über das Übergangsdatum hinaus tätig ist und seine Aktivitäten ausschließlich auf der Basis des eingereichten und noch nicht entschiedenen CASP-Antrags ausübt. Jede weitere Verzögerung erhöht das Untersagungsrisiko erheblich.

Strategie

Prof. Dr. Schwertbeck empfiehlt, die MiCAR-Zulassung als zentrales Leitmotiv der gesamten Remediation-Strategie zu behandeln. Ein überzeugender 100-Tage-Remediationsplan (vgl. 21-roadmap-remediation-100-tage.md), der alle AML- und Cyber-Mängel adressiert, ist die stärkste Argumentation für eine Zulassung trotz der Verstöße.

Quellen: dejure.org zu MiCAR Art. 143; bafin.de, Merkblatt zu MiCAR (Stand Februar 2025); BaFin-Auslegungshinweise CASP-Antrag (Januar 2025).

Datei: 04-bafin-pruefungsmitteilung-2026.md

04 — BaFin-Prüfungsmitteilung 2026

Aktenzeichen BaFin: VBS 4 1 7-K-22-188/2026

Prüfungsbezeichnung intern: Sonderprüfung 188-K-22-2026

Datum der Mitteilung: 18. März 2026

Zugang bei Thalvenia Bank AG: 18. März 2026, 09:47 Uhr (Einschreiben mit Rückschein)

Leitende Prüferin: Dr. Hannelore Kösters, BaFin Referat VBS 4

Prüfungsteam: Dr. Kösters (Leitung), Markus Pelzer (IT/Cyber), Annika Wunderwald (AML), Rolf Sandkamp (Marktintegrität)

Inhalt der Prüfungsmitteilung (Zusammenfassung)

Die BaFin ordnet auf der Grundlage von § 44 Abs. 1 KWG i.V.m. § 44c KWG eine Sonderprüfung der Thalvenia Bank AG an. Gegenstand der Prüfung sind:

1. **AML/GwG-Compliance:** Überprüfung der internen Sicherungsmaßnahmen nach §§ 4-12 GwG, insbesondere Kundensorgfaltspflichten (§ 10 GwG), verstärkte Sorgfaltspflichten (§ 15 GwG),

Verdachtsmeldepflicht (§ 43 GwG) sowie Interne Sicherungsmaßnahmen (§ 6 GwG).

2. **IT-Sicherheit / BAIT:** Überprüfung der Umsetzung der Bankaufsichtlichen Anforderungen an die IT (BAIT 2024), insbesondere Tz. 55 (Anzeigepflicht bei IT-Sicherheitsvorfällen), Notfallkonzept und Business Continuity Management.

3. **Marktintegrität / MAR:** Anlassbezogene Überprüfung des Eigenhandels der Bank in Kryptowerten, konkret in Token TN, im Zeitraum Oktober 2024 bis Januar 2026.

4. **Organisationspflichten:** Überprüfung der Umsetzung der MaRisk BA 2024, insbesondere AT 4.3 (Aufgaben- und Kompetenzverteilung) und BTO 1.1 (Kreditgeschäft, analog für Handelsgeschäfte).

Verfahrensablauf

Die BaFin kündigt folgenden Prüfungsablauf an:

Phase	Zeitraum	Inhalt
Dokumentenphase I	18.03. – 15.04.2026	Voranforderung Dokumente: AML-Handbuch, IT-Sicherheitsberichte, Handelsarchiv Token TN
Vor-Ort-Prüfung	20.04. – 30.05.2026	Prüfer-Teams in Stuttgart, Zugang zu IT-Systemen und Mitarbeiterbefragungen
Dokumentenphase II	01.06. – 30.06.2026	Nachforderung, Klärung offener Punkte
Vorläufiger Prüfbericht	ca. 30.06.2026	Übermittlung Vorentwurf an Institut
Anhörung	14.07.2026	Förmliche Anhörung gem. § 28 VwVfG
Stellungnahme	bis 28.07.2026	Frist für schriftliche Stellungnahme
Finaler Prüfbericht	ca. 15.08.2026	BaFin-Entscheidung über Maßnahmen

Dokumenten Anforderungen (Auszug)

Die BaFin fordert innerhalb von 10 Werktagen an:

- GwG-interne Sicherungsmaßnahmen-Dokumentation vollständig
- KYC-Akten für alle als Hochrisikokunden klassifizierten Kunden (Kategorie 3 und 4 gemäß internem Rating-System)
- PEP-Screening-Dokumentation der letzten 24 Monate
- STR-Meldeverzeichnis gemäß § 43 GwG
- Cybervorfall-Meldebuch und Incident-Response-Protokolle
- Handelsarchiv Token TN (Oktober 2024 bis Januar 2026)
- IT-Prüfberichte 2022-2024
- MiCAR-CASP-Antrag und Kommunikation mit BaFin WA 37

Bewertung durch die Kanzlei

Die Prüfungsmittelung lässt auf einen gut vorbereiteten, anlassbezogenen Prüfungsansatz schließen. Die BaFin hat offenkundig Vorinformationen, die zumindest drei der vier Prüfungsschwerpunkte begründen. Quelle dieser Vorinformationen ist möglicherweise:

- Eine interne Whistleblower-Meldung über das BaFin-Whistleblower-Portal
- Die verzögerte IT-Vorfallsmeldung vom Januar 2026, die trotz Verspätung schließlich bei der BaFin einging und eine Prüfung auslöste
- Handelsauffälligkeiten bei Token TN, die der BaFin-Marktüberwachung aufgefallen sind

Prof. Dr. Schwerbeck wird eine proaktive Kommunikationsstrategie mit Dr. Kösters verfolgen, um den Prüfungsablauf kooperativ zu gestalten und mögliche Untersagungsmaßnahmen zu vermeiden.

Vgl.: 05-pruefungsschwerpunkte-aml-cybersecurity.md, 12-bafin-anhoerung-juli-2026.md

Datei: 05-pruefungsschwerpunkte-aml-cybersecurity.md

05 — Prüfungsschwerpunkte AML und Cybersicherheit

Bezug: BaFin-Prüfung VBS 4 1 7-K-22-188/2026

Dokument: Interne Auswertung Kanzlei SR-2026-FIN-0612

Datum: 25. März 2026

Schwerpunkt 1: AML/GwG-Compliance

Prüferkatalog AML (BaFin-Standard)

Die BaFin verwendet für Kryptoverwahrungsunternehmen einen spezifischen AML-Prüfkatalog, der seit 2023 um MiCAR- und TFR-spezifische Anforderungen erweitert wurde. Folgende Prüfbereiche sind für Thalvenia besonders relevant:

a) Risikoanalyse (§ 5 GwG): Das Institut muss eine aktuelle, dokumentierte und vorstandsgenehmigte Risikoanalyse vorhalten. Die interne Risikoanalyse der Thalvenia datiert aus November 2023; eine Aktualisierung für 2024/2025 fehlt. Das Institut hat das verwaltete Kundenvermögen von EUR 3,1 Mrd. (Ende 2023) auf EUR 4,3 Mrd. (März 2026) gesteigert — ohne entsprechende Anpassung der Risikoanalyse.

b) Kundensorgfaltspflichten (§§ 10-14 GwG): Jeder Neukunde muss identifiziert werden; bei Hochrisikokunden sind verstärkte Sorgfaltspflichten nach § 15 GwG anzuwenden. BaFin-Prüfer haben im Vorab-Interview signalisiert, dass sie KYC-Akten für mindestens acht Hochrisikokunden untersuchen wollen.

c) PEP-Screening (§ 10 Abs. 1 Nr. 4, § 15 Abs. 3 GwG): Politisch exponierte Personen (PEP) unterliegen verschärften Anforderungen. Das Institut nutzt eine externe Datenbank (SymphonyAI Sensa); diese wurde jedoch seit 2022 nicht vertraglich auf PEP-Abdeckung für Osteuropa und Kryptowirtschaft aktualisiert.

d) Verdachtsmeldepflicht (§ 43 GwG): Im Prüfzeitraum (Oktober 2024 bis Januar 2026) wurden laut internem Meldeverzeichnis drei Verdachtsmeldungen an die FIU erstattet. Die BaFin prüft, ob weitere

Meldungen hätten erstattet werden müssen, insbesondere im Zusammenhang mit Transaktionen des Hochrisikokunden HR-07 (Token TN).

Schwerpunkt 2: IT-Sicherheit / BAIT

BAIT 2024 — Prüfungsfragen

Die Bankaufsichtlichen Anforderungen an die IT (BAIT) in der Fassung 2024 formulieren in Tz. 55 die Pflicht zur unverzüglichen Meldung wesentlicher IT-Sicherheitsvorfälle an die BaFin. "Unverzüglich" wird von der BaFin als "ohne schuldhaftes Zögern, spätestens binnen 24 Stunden nach Kenntniserlangung" ausgelegt.

Cybervorfall Januar 2026: Am 9. Januar 2026, 02:17 Uhr, wurde ein Ransomware-Angriff auf das Thalvenia-Rechenzentrumssystem festgestellt. Die Erstmeldung an die BaFin erfolgte am 13. Januar 2026 — mithin rd. 96 Stunden nach Kenntniserlangung. Dies ist ein klares Fristversäumnis nach BAIT Tz. 55. Die BaFin wertet dies als erhebliche Pflichtverletzung.

Weitere BAIT-Schwachstellen:

- Notfallkonzept (BAIT Tz. 49-54) zuletzt aktualisiert Oktober 2022; nicht MiCAR-konform.
- Business Continuity Management: DR-Tests für das MPC-Signing-System wurden seit 18 Monaten nicht durchgeführt.
- IT-Prüfbericht 2024 fehlt (Auflage aus Zulassung 2020, vgl. 02-historische-kryptoverwahrungslizenz-2020.md).

Schwerpunkt 3: Marktintegrität

Die BaFin-Prüfteammitglieder haben Rolf Sandkamp (Marktintegrität) einem gesonderten Prüfungsbereich zugewiesen, der sich um Handelsaktivitäten der Bank in Token TN dreht. Dieser Schwerpunkt hängt zusammen mit dem FIU-Verfahren (vgl. 10-suspicious-transaction-reports-fiu.md) und dem MAR-Marktmissbrauchsvorwurf (vgl. 11-mar-marktmissbrauch-vorwurf-token-tn.md).

Schwerpunkt 4: Organisationspflichten MaRisk

Die MaRisk BA 2024 (BaFin-Rundschreiben 05/2024 BA) gelten für Kreditinstitute i.S.d. KWG, also auch für Thalvenia. Die Prüfer haben signalisiert, dass sie folgende Bereiche untersuchen:

- AT 4.3.2: Klare Aufgaben- und Kompetenzverteilung; insbesondere die Abgrenzung zwischen CCO (Compliance/AML) und CRO (Risiko) in Bezug auf Kryptoverwahrungsrisiken.
- AT 7.1: Strategischer Rahmen IT (konsistent mit BAIT).
- BTO 3: Geschäftsbezogene Anforderungen an Handelsgeschäfte — erstmals auf Kryptowertehandel angewendet.

Gesamtbewertung

Das Prüfungsprogramm ist umfassend und das Risiko einer erheblichen Beanstandung hoch. Nach erster Einschätzung der Kanzlei ist mit mindestens einem schwerwiegenden Befund (BAIT/Cybervorfall), einem mittelschweren Befund (KYC/PEP) und einem noch unklaren Befund (MAR/Token TN) zu rechnen. Die Remediation-Strategie muss alle Schwerpunkte adressieren, bevor der Anhörungstermin am 14. Juli 2026 stattfindet.

06 — Cybervorfall Januar 2026 und BAIT-Meldung

Vorfalldatum: 9. Januar 2026, 02:17 Uhr (Erstalarm im SIEM-System)

Intern klassifiziert: IT-Notfall Stufe 2 (von 3)

Erstmeldung an BaFin: 13. Januar 2026, 14:32 Uhr

Meldungsverzug: rd. 96 Stunden (4 Tage)

Technischer Sachverhalt

In der Nacht vom 8. auf den 9. Januar 2026 infiltrierten unbekannte Angreifer das Netzwerk der Thalvenia Bank AG über eine ungepatchte Schwachstelle im VPN-Gateway (Fortinet FortiGate, CVE-2024-21762). Die Angreifer erlangten zunächst Zugang zu einem Segment des internen Netzwerks, das die Verwaltungssoftware für das Cold-Custody-System hostet.

Ablauf des Vorfalls:

Zeit	Ereignis
09.01.2026, 02:17	SIEM-Alarm: ungewöhnlicher Zugriff VPN-Gateway
09.01.2026, 02:45	SOC (Schichtbetrieb) stuft als False Positive ein; keine Eskalation
09.01.2026, 08:10	Ransomware-Deployment entdeckt; 14 Server verschlüsselt
09.01.2026, 08:30	CISO Magnus Thorvaldsson informiert; IT-Notfall Stufe 2 ausgerufen
09.01.2026, 10:00	COO Marc Vellbruck informiert
09.01.2026, 13:00	Vollständige Vorstandsinfo; Isolierung infizierter Segmente
09.01.2026, 16:00	Forensik-Team extern mandatiert (CyberTrust GmbH, Frankfurt)
10.-12.01.2026	Forensische Analyse und Eindämmungsmaßnahmen
13.01.2026, 14:32	BaFin-Meldung über BAIT-Meldeportal

BAIT-Meldepflicht und Fristversäumnis

Rechtsgrundlage: BAIT 2024, Tz. 55: "Institute haben wesentliche IT-Sicherheitsvorfälle der Aufsicht unverzüglich anzuzeigen."

Die BaFin-Verwaltungspraxis definiert "unverzüglich" unter Rückgriff auf § 121 BGB analog als "ohne schuldhaftes Zögern, d.h. spätestens 24 Stunden nach Kenntniserlangung eines wesentlichen IT-Sicherheitsvorfalls." Zusätzlich verweist Tz. 55 BAIT auf die EBA-Leitlinien zu ICT- und Sicherheitsrisikomanagement (EBA/GL/2019/04), die eine Erstmeldung innerhalb von 4 Stunden nach Klassifizierung als wesentlich vorsehen.

Sachverhaltsanalyse:

- Kenntniserlangung für BAIT-Zwecke: spätestens 9. Januar 2026, 08:30 Uhr (CISO informiert).
- Meldung erfolgte: 13. Januar 2026, 14:32 Uhr.

- Verzug: 78 Stunden nach Pflichtbeginn (CISO-Kenntniserlangung), 30 Stunden nach Vollständiger-Vorstandskennntnis.

Der Meldungsverzug ist schwerwiegend. Das Institut beruft sich auf die laufende forensische Analyse, die abgewartet werden sollte, um der BaFin einen vollständigen Sachverhalt zu melden. Dieses Argument ist aufsichtsrechtlich schwach, da BAIT Tz. 55 ausdrücklich eine Erstmeldung mit den zum Zeitpunkt bekannten Informationen und Folgemeldungen bei fortschreitender Aufklärung vorsieht.

Schadensumfang

- 14 Server des Verwaltungsnetzwerks verschlüsselt (keine Hot-Wallet-Systeme betroffen)
- Kundenfonds zu keinem Zeitpunkt gefährdet (Cold-Custody physisch getrennt)
- Produktionsausfall MPC-Signing-Service: 18 Stunden (9./10. Januar 2026)
- Keine Datenabrufanfragen von Kunden unerfüllt geblieben
- Forensik identifizierte: Angreifer hatten keinen Zugriff auf private Schlüssel
- Lösegeldforderung: 35 Bitcoin; Zahlung verweigert; Daten aus Backup wiederhergestellt

Folgemaßnahmen (nach Vorfall)

1. Notfall-Patch FortiGate VPN-Gateway (10. Januar 2026, abgeschlossen)
2. Netzwerksegmentierung verschärft; Produktions- und Verwaltungsnetz strikter getrennt
3. SOC-Eskalationsprozesse überarbeitet; neues Runbook "IT-Notfall Stufe 1-3" erlassen
4. BAIT-Meldung nachgeholt (13. Januar 2026)
5. Nachträgliche Meldung auch an BSI nach BSIG (erfolgte parallel)

Bewertung durch BaFin-Prüfer

Im Prüfungsgespräch vom 5. Mai 2026 qualifizierte Prüferin Dr. Kösters den Meldungsverzug als "schwerwiegende Pflichtverletzung nach BAIT Tz. 55", die isoliert ein Bußgeld nach § 56 GwG (sofern als Aufsichtsrechtsverletzung behandelt) oder eine Anordnung nach § 25a KWG rechtfertigen könne. Die Kanzlei bereitet eine Entlastungsargumentation vor, die auf die erstmalige Klassifizierungsunsicherheit und den bereits abgeschlossenen Remediation-Status abstellt.

Vgl.: 17-sanktionsrahmen-bussgeld-untersagung.md, 13-stellungnahme-vorstand-thalvenia.md

Datei: 07-aml-pflichten-gwg-katalog.md

07 — AML-Pflichtenkatalog nach GwG

Bezug: BaFin-Prüfung VBS 4 1 7-K-22-188/2026

Prüferin AML: Annika Wunderwald, BaFin Referat GW 2

Internes Kanzleidokument: SR-2026-FIN-0612-AML-01

Übersicht GwG-Pflichten und Befunde

GwG-Pflicht	Paragraph	Status Thalvenia	Befund BaFin
Risikoanalyse	§ 5 GwG	Risikoanalyse vorhanden, aber veraltet (2023)	Wesentlicher Befund: keine Aktualisierung 2024/2025
Organisatorische Pflichten	§ 6 GwG	CCO bestellt; Schulungsplan vorhanden	Befund: Schulungsplan nicht vollständig umgesetzt
Beauftragtenbenennung	§ 7 GwG	CCO Dr. Tannenfels als Geldwäschebeauftragter benannt	Befund: Vertretungsregelung unzureichend
Allgemeine Sorgfaltspflichten	§ 10 GwG	KYC-Prozess existiert	Wesentlicher Befund: 8 Hochrisikokunden unvollständig
Vereinfachte Sorgfaltspflichten	§ 14 GwG	Kategorisierung vorhanden	Kein Befund
Verstärkte Sorgfaltspflichten	§ 15 GwG	Nur teilweise angewandt	Wesentlicher Befund: PEP-Screening-Lücken
Transaktionsmonitoring	§ 25h KWG (analog)	Softwarelösung Chainalysis Reactor vorhanden	Befund: Regelwerk seit 2022 nicht aktualisiert
Verdachtsmeldepflicht	§ 43 GwG	3 Meldungen 2024-2026	Wesentlicher Befund: Unterlassene Meldungen
Aufbewahrungspflichten	§ 8 GwG	Archiv vorhanden	Kein Befund
Datenschutz-AML-Abwägung	§ 11 Abs. 6 GwG	Policy vorhanden	Kein Befund

Detailanalyse der wesentlichen Befunde

Befund 1: Veraltete Risikoanalyse (§ 5 GwG)

Die letzte genehmigte Risikoanalyse datiert vom 12. November 2023. Das GwG und die BaFin-Auslegungshinweise verlangen eine anlassbezogene Aktualisierung, mindestens jedoch jährlich. Im Jahr 2024 gab es zwei wesentliche Auslöser für eine Aktualisierung:

- Einführung des MiCAR-Übergangsregimes (neues Geschäftsmodell)
- Aufnahme des Eigenhandels in Token TN (Oktober 2024)

Keine Aktualisierung der Risikoanalyse ist erfolgt. Die Prüferin bewertet dies als eigenständigen wesentlichen Mangel.

Befund 2: Unvollständige KYC-Akten (§ 10 GwG)

Von 47 als Hochrisikokunden klassifizierten Kunden (Kategorie 3 oder 4) wurden acht durch die BaFin-Prüferin für eine Stichprobenprüfung ausgewählt. Bei vier dieser acht Kunden wurden wesentliche

Mängel in der KYC-Dokumentation festgestellt:

- Kunden HR-03: Wirtschaftlich Berechtigter nicht festgestellt (§ 3 Abs. 1 GwG)
- Kunden HR-07: Herkunft der Fondsmittel nicht dokumentiert (§ 15 Abs. 4 GwG)
- Kunden HR-11: PEP-Status nicht erkannt (vgl. 09-pep-screening-fehler.md)
- Kunden HR-19: Aktualisierungsintervall 4 Jahre überschritten (§ 10 Abs. 3 GwG)

Vgl. hierzu ausführlich 08-kundenidentifikation-kyc-mangel.md.

Befund 3: Verdachtsmeldungen (§ 43 GwG)

Die BaFin-Prüferin hat im Transaktionsmonitoring-System für den Zeitraum Oktober 2024 bis Januar 2026 17 Transaktionen mit Auffälligkeitsindikatoren identifiziert, von denen lediglich drei zur Verdachtsmeldung an die FIU geführt haben. Die verbleibenden 14 Transaktionen wurden intern mit kurzen Vermerken dokumentiert und nicht gemeldet.

Für die fünf Transaktionen mit den höchsten Risikowerten empfahl die Prüferin eine Nachprüfung, ob eine Meldepflicht nach § 43 GwG hätte ausgelöst werden müssen. Zwei dieser Transaktionen betreffen Kunde HR-07 und haben direkten Bezug zum MAR-Verfahren Token TN.

Interne AML-Organisation

- Geldwäschebeauftragter: CCO Dr. Lasse Tannenfels (gleichzeitig strafverdächtig wegen § 261 StGB — problematisch)
- Stellvertreter: Lena Göbel-Strauch, AML-Analystin (ohne formelle GMLB-Ausbildung)
- AML-Team: 4 Vollzeitstellen (für EUR 4,3 Mrd. AuM nach BaFin-Einschätzung zu wenig)
- Schulungsquote 2025: 68 % der AML-relevanten Mitarbeiter (Ziel: 100 %)

GwG-Bußgeldrelevanz

§ 56 GwG sieht für Verstöße gegen die Pflichten der §§ 10-15 GwG Bußgelder bis zu EUR 5 Mio. (oder 10 % des Umsatzes, falls höher) vor. § 60b GwG ermächtigt zur Veröffentlichung von Bußgeldbescheiden bei Kreditinstituten. Die Gesamtbewertung der AML-Mängel könnte nach Einschätzung der Kanzlei zu einem Bußgeld im Bereich EUR 800.000 bis EUR 2,5 Mio. führen.

Vgl.: [xlsx/gwg-pflichten-katalog.xlsx](#) für die tabellarische Gesamtübersicht mit Fristen und Maßnahmen.

Datei: 08-kundenidentifikation-kyc-mangel.md

08 — Kundenidentifikation und KYC-Mängel

Prüfungsgegenstand: Kundensorgfaltspflichten gem. §§ 10-15 GwG

Stichprobe BaFin: 8 Hochrisikokunden (Kategorie 3 und 4)

Untersuchungszeitraum: Onboarding bis März 2026

Methodische Grundlage

Die BaFin-Prüferin Annika Wunderwald führte eine risikobasierte Stichprobenprüfung durch. Die acht Kunden wurden nach folgenden Kriterien ausgewählt:

- Kundenkategorie 3 oder 4 (Hochrisiko)
- Transaktionsvolumen über EUR 1 Mio. in den letzten 12 Monaten
- Kundendomizil in Ländern mit erhöhtem Geldwäscherisiko (FATF Grey List oder Hochrisikodrittland)

Ergebnisse der Stichprobenprüfung

Kunde HR-01 (Investmentgesellschaft, Dubai)

- **Risikoklasse:** 4
- **KYC-Status:** Grundidentifizierung vorhanden
- **Befund:** Wirtschaftlich Berechtigte korrekt identifiziert; aktuelles Organigramm fehlt (letzte Aktualisierung März 2023).
- **Mangel:** Mittelschwer — Aktualisierungspflicht § 10 Abs. 3 GwG verletzt.

Kunde HR-03 (Einzelperson, Zypern)

- **Risikoklasse:** 4
- **KYC-Status:** Kritische Lücke
- **Befund:** Wirtschaftlich Berechtigter gemäß § 3 Abs. 1 GwG nicht festgestellt. Transaktionen i.H.v. EUR 3,2 Mio. wurden ohne vollständige WiB-Feststellung abgewickelt.
- **Mangel:** Schwerwiegend — Kernpflicht nach § 10 Abs. 1 Nr. 2 GwG verletzt.

Kunde HR-05 (Family Office, Luxemburg)

- **Risikoklasse:** 3
- **KYC-Status:** Weitgehend vollständig
- **Befund:** PEP-Screening ergab keinen Treffer; interne Dokumentation lückenlos.
- **Mangel:** Kein wesentlicher Befund; Aktualisierungsintervall ordnungsgemäß.

Kunde HR-07 (Stiftung, Liechtenstein)

- **Risikoklasse:** 4
- **KYC-Status:** Kritische Lücke
- **Befund:** Herkunft der eingebrachten Fondsmittel (EUR 18,7 Mio.) nicht hinreichend dokumentiert. Vorliegende Unterlagen beschränken sich auf eine einseitige Erklärung des Stiftungsrats ohne Belege. Zugleich ist dieser Kunde Partei von Transaktionen, die im MAR-Kontext relevant sind (Token TN).
- **Mangel:** Schwerwiegend — § 15 Abs. 4 GwG (verstärkte Sorgfaltspflichten: Herkunft der Mittel) verletzt.

Kunde HR-09 (Kryptounternehmen, El Salvador)

- **Risikoklasse:** 4
- **KYC-Status:** Lückenhaft
- **Befund:** El Salvador ist seit 2021 auf der FATF-Beobachtungsliste. Verstärkte Sorgfaltspflichten nach § 15 Abs. 3 Nr. 2 GwG hätten angewendet werden müssen. Tatsächlich wurden nur allgemeine Sorgfaltspflichten durchgeführt.

- **Mangel:** Schwerwiegend — Länderspezifische Hochrisikoeinstufung nicht berücksichtigt.

Kunde HR-11 (Einzelperson, Georgien)

- **Risikoklasse:** 3 (bei Onboarding)
- **KYC-Status:** PEP-Fehler
- **Befund:** Der Kunde ist ein ehemaliger Ministerialbeamter Georgiens. Er wurde beim Onboarding 2022 nicht als PEP erkannt; das PEP-Screening-System von SymphonyAI enthält keine Einträge für mittlere Positionen in der georgischen Ministerialverwaltung. Nachträglich durch Pressebericht identifiziert.
- **Mangel:** Schwerwiegend — § 15 Abs. 3 Nr. 1 GwG (PEP-Feststellung) verletzt. Vgl. 09-pep-screening-fehler.md.

Kunde HR-15 (Investmentfonds, Cayman Islands)

- **Risikoklasse:** 3
- **KYC-Status:** Weitgehend vollständig
- **Befund:** Cayman Islands sind Hochrisikodrittland i.S.v. § 15 Abs. 3 Nr. 2 GwG. Verstärkte Sorgfaltspflichten wurden korrekt angewendet, jedoch fehlt die Genehmigung durch die Geschäftsleitung (§ 15 Abs. 5 Nr. 2 GwG).
- **Mangel:** Mittelschwer — Formverletzung.

Kunde HR-19 (Hedgefonds, Singapur)

- **Risikoklasse:** 3
- **KYC-Status:** Veraltet
- **Befund:** Letzte vollständige KYC-Aktualisierung: August 2021. Aktualisierungsintervall von 24 Monaten (interne Richtlinie) stark überschritten. Umfangreiche Transaktionen (EUR 8,4 Mio. in 2025) ohne aktuelle KYC-Basis.
- **Mangel:** Schwerwiegend — § 10 Abs. 3 S. 4 GwG (Aktualisierungspflicht) verletzt.

Zusammenfassung Befundübersicht

Kunde	Risikoklasse	Hauptmangel	Schweregrad
HR-01	4	Veraltetes Organigramm	Mittel
HR-03	4	WiB nicht festgestellt	Schwer
HR-05	3	Kein wesentlicher Befund	-
HR-07	4	Mittelherkunft unklar	Schwer
HR-09	4	Länderspezifische Hochrisikoprüfung unterblieben	Schwer
HR-11	3	PEP nicht erkannt	Schwer
HR-15	3	GF-Genehmigung fehlt	Mittel
HR-19	3	KYC veraltet (5 Jahre)	Schwer

5 von 8 Kunden: schwerwiegende Mängel. Dieser Befund wird nach Einschätzung der Kanzlei im Anhörungsverfahren besonderes Gewicht haben.

Vgl.: xlsx/kundenidentifikation-kyc-mangelpruefung.xlsx

Datei: 09-pep-screening-fehler.md

09 — PEP-Screening-Fehler

Rechtsgrundlage: § 10 Abs. 1 Nr. 4, § 15 Abs. 3 Nr. 1, Abs. 5 GwG; BaFin-Auslegungshinweise GwG (Oktober 2021)

Betroffene Kunden: HR-11 (Georgien), HR-23 (Moldau), HR-31 (Nordmazedonien)

PEP-Screening-Anbieter: SymphonyAI Sensa (Vertrag seit 2021, zuletzt aktualisiert Oktober 2022)

Rechtlicher Rahmen

Politisch exponierte Personen (PEP) i.S.d. § 1 Abs. 12 GwG unterliegen nach § 15 Abs. 3 Nr. 1 GwG verschärften Anforderungen. Dazu zählen:

- Einholung der Zustimmung der Geschäftsleitung vor Begründung der Geschäftsbeziehung (§ 15 Abs. 5 Nr. 2 GwG)
- Feststellung der Herkunft der eingesetzten Vermögenswerte (§ 15 Abs. 5 Nr. 3 GwG)
- Laufende, verstärkte Überwachung der Geschäftsbeziehung (§ 15 Abs. 5 Nr. 4 GwG)

Der Begriff "PEP" umfasst nach § 1 Abs. 12 Nr. 4 GwG auch Mitglieder von Leitungsorganen staatseigener Unternehmen sowie deren unmittelbare Familienangehörige (§ 1 Abs. 13 GwG) und bekannte enge Mitarbeiter (§ 1 Abs. 14 GwG).

Technische Ursache des Screening-Fehlers

Das SymphonyAI-Sensa-System wird von Thalvenia für alle Kunden beim Onboarding und danach jährlich eingesetzt. Der Vertrag mit SymphonyAI sieht folgende Leistungen vor:

- Weltweite PEP-Datenbank: Tier 1 (Staatsoberhäupter, Minister, Parlamentarier)
- Sanktionslisten: EU, USA (OFAC), UN, Großbritannien

Nicht enthalten: Tier 2 (Vize-Minister, Staatssekretäre, mittlere Beamtenebene, regionale Politiker nicht-westlicher Staaten). Dies betrifft besonders Länder der früheren Sowjetunion und des Balkans, wo PEP-Definitionen breiter sind und die BaFin-Auslegungshinweise eine entsprechend erweiterte Datenabdeckung verlangen.

Einzelfälle

Kunde HR-11 — Georgischer Ministerialbeamter

- Onboarding: März 2022
- Funktion bei Onboarding: Leiter der Abteilung für Haushalt und Finanzen im georgischen Wirtschaftsministerium (Ministerialebene II, nicht Tier 1)

- PEP-Screening-Ergebnis 2022: "Kein Treffer"
- Entdeckung: August 2025, durch Pressebericht (Ermittlungsverfahren in Georgien)
- Nachträgliche Einschätzung: PEP-Status nach § 1 Abs. 12 Nr. 4 GwG seit Onboarding gegeben

Konsequenz: Sämtliche Transaktionen seit März 2022 (EUR 6,3 Mio.) wurden ohne GF-Genehmigung und ohne verstärkte Überwachung abgewickelt.

Kunde HR-23 — Moldauischer Bürgermeister a.D.

- Onboarding: Juli 2023
- Funktion: Ehemaliger Bürgermeister einer Stadt mit über 50.000 Einwohnern (Moldova); amtlich bis 2021
- PEP-Screening-Ergebnis 2023: "Kein Treffer"
- Technische Ursache: Bürgermeister mittelgroßer Städte in Moldova nicht in Tier-1-Datenbank erfasst
- Nachträgliche Einschätzung: PEP-Status nach § 1 Abs. 12 Nr. 5 GwG (kommunale Leitungsorgane)

Kunde HR-31 — Nordmazedonischer Richter am Obersten Gericht

- Onboarding: Januar 2024
- Funktion: Aktiver Richter am Obersten Gericht Nordmazedoniens
- PEP-Screening-Ergebnis 2024: "Kein Treffer"
- Technische Ursache: Justizbehörden Nordmazedoniens nicht in Tier-1-Datenbank
- Nachträgliche Einschätzung: PEP-Status nach § 1 Abs. 12 Nr. 6 GwG (leitende Mitglieder der Judikative)

Bewertung durch BaFin

Prüferin Wunderwald beurteilte die drei PEP-Fälle als systematischen Mangel, nicht als Einzelversagen. Das Institut hätte bei Aufnahme von Geschäftsbeziehungen mit natürlichen Personen aus osteuropäischen Ländern mit erhöhtem Korruptionsrisiko (CPI-Score < 45) proaktiv eine erweiterte Datenbank verwenden müssen.

Die BaFin verweist auf ihre Auslegungshinweise GwG (Oktober 2021), Abschnitt zu § 1 Abs. 12, wonach Institute verpflichtet sind, die Qualität der verwendeten PEP-Datenbanken risikoadäquat zu prüfen und ggf. mehrere Datenbanken zu kombinieren.

Sofortmaßnahmen (Remediation)

1. Upgrade SymphonyAI-Sensa-Vertrag auf Tier-1 + Tier-2-Abdeckung (beauftragt April 2026).
2. Retrograde PEP-Überprüfung aller Hochrisikokunden aus Tier-2-relevanten Ländern (abgeschlossen Mai 2026).
3. Drei betroffene Kunden: formelle Nacherfüllung der PEP-Pflichten; GF-Genehmigungen nachgeholt; verstärkte Überwachung aktiviert.
4. Compliance-Schulung PEP-Erkennung: alle AML-relevanten Mitarbeiter (Juni 2026).

Vgl.: 08-kundenidentifikation-kyc-mangel.md; 07-aml-pflichten-gwg-katalog.md

Datei: 10-suspicious-transaction-reports-fiu.md

10 — Suspicious Transaction Reports und FIU-Verfahren

Rechtsgrundlage: § 43 GwG (Verdachtsmeldepflicht); § 44 GwG (Verbot der Informationsweitergabe)

FIU-Aktenzeichen: 2026-FIU-7711-TN

FIU-Auskunftersuchen: 22. Februar 2026

Antwort Thalvenia: 15. März 2026 (über Kanzlei)

Hintergrund

Die Financial Intelligence Unit (FIU) Deutschland ist als Zentralstelle für Finanztransaktionsuntersuchungen (§ 27 GwG) zuständig für die Entgegennahme, Analyse und Weiterleitung von Verdachtsmeldungen nach § 43 GwG. Sie ist organisatorisch beim Bundeszollamt angesiedelt.

Im Februar 2026 wandte sich die FIU mit einem Auskunftersuchen an die Thalvenia Bank AG. Hintergrund war eine Auswertung des FIU-Analysesystems (goAML), das Transaktionsmuster im Zusammenhang mit Token TN als potenziell geldwäscherelevant identifiziert hatte. Das FIU-Verfahren ist von der BaFin-Sonderprüfung zu unterscheiden, läuft aber parallel.

FIU-Auskunftersuchen (Zusammenfassung)

Das FIU-Ersuchen vom 22. Februar 2026 bezieht sich auf Transaktionen im Zeitraum Oktober 2024 bis Januar 2026. Es fragt ab:

- 1. Sämtliche Transaktionsdaten für Token TN aller Kunden
- 2. KYC-Dokumentation für Kunden HR-07 und HR-11
- 3. Ob und wann Verdachtsmeldungen zu diesen Kunden erstattet wurden
- 4. Interne Risikoklassifizierung beider Kunden
- 5. Kommunikation zwischen dem Institut und diesen Kunden (transaktionsbezogen)

Verdachtsmeldungen (§ 43 GwG) — Gesamtübersicht

Im Prüfungszeitraum erstattete Thalvenia drei Verdachtsmeldungen:

Meldungs-Nr.	Datum	Kunde	Transaktions betrag	Verdachtsgru nd	FIU-Bestätig ung
STR-2025-001	12. März 2025	HR-07	EUR 2,1 Mio.	Ungewöhnlic he Herkunft	15. März 2025
STR-2025-002	30. August 2025	Nicht offenbart	EUR 450.000	Verschleieru ngsstruktur	02. September 2025
STR-2026-001	18. Januar 2026	HR-11	EUR 680.000	Sanktionslist en-Treffer (N achtragsscre ening)	21. Januar 2026

Unterlassene Verdachtsmeldungen — Befund BaFin

Die BaFin-Prüferin identifizierte im Transaktionsmonitoring-System 14 weitere Transaktionen mit automatisch erzeugten Auffälligkeitshinweisen (Flags), die nicht zur Meldung führten. Für fünf davon empfiehlt die Prüferin eine Prüfung, ob eine Meldepflicht ausgelöst wurde:

Flagge	Datum	Kunde	Betrag	Auffälligkeit	Interne Entscheidung	BaFin-Einschätzung
TRX-2024-0487	15.10.2024	HR-07	EUR 1,8 Mio.	Rapid movement aus Cold Wallet	Kein Verdacht (interner Vermerk)	Meldepflicht möglicherweise ausgelöst
TRX-2024-0612	22.11.2024	HR-07	EUR 3,4 Mio.	Splitting-Muster	Kein Verdacht	Meldepflicht möglicherweise ausgelöst
TRX-2025-0089	10.02.2025	HR-03	EUR 900.000	Ursprung Darknet-assoziierte Adressen	"Falsch positiv"	Befund schwerwiegend
TRX-2025-0341	05.06.2025	HR-19	EUR 4,1 Mio.	Wirtschaftlicher Zweck unklar	Kein Verdacht	Meldepflicht möglicherweise ausgelöst
TRX-2026-0044	07.01.2026	HR-07	EUR 2,2 Mio.	Zeitnahe Token-TN-Transaktionen (Pre-Cyberfall)	Nicht bewertet	Zusammenhang mit MAR-Verfahren

Verbot der Informationsweitergabe (§ 44 GwG)

Die Kanzlei weist darauf hin, dass die laufenden FIU-Ermittlungen unter das Tipping-off-Verbot des § 44 GwG fallen. Kunden dürfen nicht darüber informiert werden, dass gegen sie oder ihre Transaktionen eine Verdachtsmeldung erstattet wurde oder dass die FIU ermittelt. Dies schränkt die Kommunikation mit den betroffenen Kunden erheblich ein.

Im Fall der Kunden HR-07 und HR-11 wurde sichergestellt, dass keine Informationen über die FIU-Anfrage nach außen gedrungen sind.

Bewertung und Risiko

Die FIU hat in ihrem Ersuchen signalisiert, dass bei einer Weiterleitung der Informationen an Strafverfolgungsbehörden (§ 32 GwG) eine Strafverfolgung wegen § 261 StGB (Geldwäsche) gegen Verantwortliche des Instituts — nicht nur gegen CCO Dr. Tannenfels — möglich sei. Dies erhöht den Druck auf das Institut erheblich.

Vgl.: 16-individual-strafverfahren-vorstand.md; 11-mar-marktmissbrauch-vorwurf-token-tn.md

11 — MAR-Marktmissbrauchsvorwurf Token TN

Rechtsgrundlage: Verordnung (EU) 596/2014 (MAR), insb. Art. 15 (Marktmanipulationsverbot); MiCAR Art. 89-92 (Marktmissbrauchsregeln für Kryptowerte)

Betroffenes Instrument: Token TN (Utility-Token, nicht als Wertpapier klassifiziert; MiCAR-spezifisches Instrument)

BaFin-Prüfer: Rolf Sandkamp, BaFin Referat WA 23 (Marktüberwachung)

Relevanter Zeitraum: Oktober 2024 bis Januar 2026

Token TN — Hintergrund

Token TN ist ein Utility-Token eines deutschen Startups, der auf der Ethereum-Blockchain ausgegeben wird. Thalvenia Bank AG hat im Oktober 2024 begonnen, Token TN im eigenen Namen zu handeln (Eigenhandel). Gleichzeitig verwahrt das Institut Token TN für vier institutionelle Kunden, darunter Kunde HR-07.

Da Token TN keinem regulierten Handelsplatz i.S.d. MiFID II unterliegt, gelten die MAR-Regeln für Finanzinstrumente (Art. 2 Abs. 1 MAR) nicht unmittelbar. Jedoch gilt seit 30. Dezember 2024 Art. 89 MiCAR, der ein eigenständiges Marktmissbrauchsregime für Kryptowerte normiert, welches inhaltlich Art. 12-15 MAR nachgebildet ist.

Vorwurf

BaFin-Prüfer Sandkamp hat im Rahmen der Vor-Ort-Prüfung Handelsarchivdaten ausgewertet. Seine vorläufige Einschätzung (Prüfungsgespräch 22. Mai 2026):

Der Eigenhandel der Thalvenia Bank in Token TN zeigt für den Zeitraum November bis Dezember 2024 Muster, die auf koordinierte Kaufaufträge hindeuten könnten, die in Kombination mit Kaufaufträgen des Kunden HR-07 den Kurs von Token TN beeinflussen. Konkret:

- **Zeitraum 15.-22. November 2024:** Thalvenia kauft intern Token TN im Wert von EUR 4,2 Mio. Gleichzeitig kauft HR-07 (über Thalvenia als Verwahrer) Token TN im Wert von EUR 3,8 Mio.
- **Kurseffekt:** Token TN steigt in diesem Zeitraum um 38 %.
- **Zeitraum 5.-12. Dezember 2024:** Thalvenia verkauft intern Token TN im Wert von EUR 6,1 Mio. (teilweise Gewinnmitnahme). HR-07 hält Position.
- **Zeitraum 20.-27. Januar 2026:** HR-07 liquidiert Position in Token TN vollständig (EUR 18,7 Mio. Erlös). Kurs fällt danach um 42 %.

Rechtliche Einordnung

Nach Art. 89 Abs. 2 MiCAR ist Marktmanipulation bei Kryptowerten verboten. Das konkrete Verbotssmerkmal "Meinungsäußerungen oder Beurteilungen, durch die Irreführungen entstehen oder wahrscheinlich entstehen" (Art. 89 Abs. 2 lit. c MiCAR) sowie "Transaktionen oder Aufträge, durch die falsche oder irreführende Signale gegeben werden" (Art. 89 Abs. 2 lit. a MiCAR) könnten erfüllt sein.

Für die haftungsrechtliche Einordnung ist entscheidend, ob:

1. Das Institut und HR-07 koordiniert handelten (dann: gemeinsames Handeln Art. 12 MAR analog)
2. Das Institut auf eigene Rechnung handelte und dabei von Kundenaufträgen profitierte (dann: Front-Running-Variante)
3. Kein koordiniertes Handeln vorlag, aber das Institut seine Stellung als Verwahrer der HR-07-Bestände nutzte (dann: Informationsasymmetrie-Nutzung)

Interessenkonflikte und MaRisk

Die gleichzeitige Stellung als Eigenhandels-Akteur und Verwahrer/Treuhänder für Kunden in demselben Token schafft strukturelle Interessenkonflikte. Nach MaRisk AT 4.3.2 und Art. 72 MiCAR hätte das Institut diese Konflikte durch geeignete Regelungen (Chinese Walls, Verbote) ausschließen oder offenlegen müssen. Interne Prüfung ergibt: Es existiert ein allgemeines Interessenkonflikt-Policy-Dokument, das jedoch Kryptowerte-Eigenhandel nicht explizit adressiert.

Strafrechtsrelevanz

Art. 15 MAR analog (über Art. 89 MiCAR) kann bei nachgewiesener Marktmanipulation zu einer Strafanzeige führen. In Deutschland ist Marktmanipulation nach § 119 WpHG strafbar (Freiheitsstrafe bis zu 4 Jahren). Für Kryptowerte gilt seit FinmadiG-Umsetzung ein analoges Regime.

Darüber hinaus besteht wegen des Zusammenhangs mit Kunde HR-07 (unklare Mittelherkunft, FIU-STR) ein erhebliches Geldwäscherisiko (§ 261 StGB), das die Strafverfolgung gegen CCO Dr. Tannenfels antreibt.

Status und Nächste Schritte

BaFin-Referat WA 23 hat mitgeteilt, dass eine formelle Marktmissbrauchs-Untersuchung nach Art. 89 MiCAR noch nicht eingeleitet wurde. Der Befund befindet sich in der Voruntersuchungsphase. Die Kanzlei bereitet eine Einlassung vor, die das Fehlen einer Koordinationsabrede und die eigenständige, ökonomisch rationale Handelslogik des Instituts darstellt.

Vgl.: 10-suspicious-transaction-reports-fiu.md; 18-strategie-vergleichsangebot-bafin.md

Datei: 12-bafin-anhoerung-juli-2026.md

12 — BaFin-Anhörung Juli 2026

Aktenzeichen: BaFin VBS 4 1 7-K-22-188/2026

Anhörungsschreiben: 14. Juli 2026

Frist Stellungnahme: 28. Juli 2026

Rechtsgrundlage: § 28 Abs. 1 VwVfG (rechtliches Gehör vor Erlass belastender Verwaltungsakte)

Inhalt des Anhörungsschreibens

Das Anhörungsschreiben der BaFin (unterzeichnet Dr. Hannelore Kösters, Referat VBS 4) fasst die vorläufigen Prüfungsfeststellungen zusammen und kündigt folgende beabsichtigte Maßnahmen an:

Beabsichtigte Maßnahme 1: Anordnung nach § 25a Abs. 1 KWG

Die BaFin beabsichtigt, die Thalvenia Bank AG zu verpflichten, folgende Mängel innerhalb von 60 Tagen zu beheben:

- Aktualisierung der Risikoanalyse nach § 5 GwG
- Vollständige KYC-Nacherfüllung für alle Kunden mit schwerwiegenden Befunden
- Vollständige PEP-Screening-Dokumentation und Vertragsupgrade mit SymphonyAI
- Überarbeitung des BAIT-konformen Notfallkonzepts
- Vorlage des ausstehenden IT-Prüfberichts 2024

Beabsichtigte Maßnahme 2: Bußgeldverfahren nach § 56 GwG

Die BaFin beabsichtigt, ein Bußgeldverfahren wegen folgender Verstöße einzuleiten:

- Verletzung der Sorgfaltspflichten nach § 10 GwG (für Kunden HR-03, HR-07, HR-09, HR-11, HR-19)
- Verletzung der verstärkten Sorgfaltspflichten nach § 15 GwG (für Kunden HR-11, HR-23, HR-31)
- Verletzung der Meldepflicht nach § 43 GwG (für nicht gemeldete Transaktionen TRX-2024-0487, TRX-2024-0612, TRX-2025-0089)
- Verletzung der BAIT-Anzeigepflicht (Cybervorfall Januar 2026)

Vorläufig geschätzter Bußgeldrahmen: EUR 2,5 Mio. bis EUR 5 Mio.

Beabsichtigte Maßnahme 3: Hinweis MiCAR-Zulassung

"Die festgestellten Mängel werden in die laufende Prüfung des CASP-Antrags nach Art. 63 MiCAR einfließen. Das Referat WA 37 wurde informiert. Eine abschließende Entscheidung über den CASP-Antrag wird nach Abschluss des vorliegenden Prüfungsverfahrens ergehen."

Dies ist die schärfste Formulierung des Anhörungsschreibens und impliziert die mögliche Versagung der CASP-Zulassung.

Rechtliche Analyse des Anhörungsschreibens

Zu Maßnahme 1 (§ 25a KWG-Anordnung)

Die BaFin ist befugt, nach § 25a Abs. 1 S. 7 KWG Maßnahmen anzuordnen, die geeignet und erforderlich sind, unzureichende Vorkehrungen zu beseitigen. Die Anordnung ist verhältnismäßig, sofern das Institut die Mängel beheben kann. Da das Institut seit April 2026 aktiv an der Remediation arbeitet (vgl. 21-roadmap-remediation-100-tage.md), werden wir im Rahmen der Stellungnahme nachweisen, dass viele Maßnahmen bereits abgeschlossen sind.

Zu Maßnahme 2 (Bußgeldverfahren)

§ 56 GwG sieht für Verstöße gegen §§ 10, 15 GwG Bußgelder bis zu EUR 5 Mio. vor. Der Vorwurf der unterlassenen Verdachtsmeldung nach § 43 GwG ist schwerwiegend und rechtlich am anfälligsten zu verteidigen. Die Kanzlei wird argumentieren, dass das interne Monitoring-System die fraglichen Transaktionen als Grenzfall eingestuft hat und die Entscheidung gegen eine Meldung auf einer vertretbaren Risikoeinschätzung basierte.

Zu Maßnahme 3 (MiCAR-Zulassung)

Die Verbindung zwischen Bußgeldverfahren und MiCAR-Zulassung ist der heikelste Punkt. Art. 63 Abs. 1 MiCAR erlaubt die Versagung, wenn das Institut "nicht zuverlässig und solide geführt" ist. Diese Formulierung ist vage und ermöglicht der BaFin einen weiten Ermessensspielraum. Die Stellungnahme muss überzeugend darlegen, dass das Institut trotz der Mängel die Anforderungen an eine zuverlässige Führung erfüllt.

Strategie für die Stellungnahme

Prof. Dr. Schwerbeck empfiehlt einen dreistufigen Ansatz:

1. **Sachverhaltsdarstellung:** Detaillierte, von den BaFin-Feststellungen abweichende oder ergänzende Sachverhaltsdarstellung insbesondere beim Cybervorfall-Meldungsverzug und den unterlassenen STR-Meldungen.
2. **Remediationsnachweis:** Vollständige Dokumentation aller seit März 2026 ergriffenen Maßnahmen (Fortschritt 100-Tage-Plan).
3. **Proportionalitätsargumentation:** Hinweis auf Erstverstoß, kooperatives Verhalten, fehlenden Vorsatz und bereits abgeschlossene Remediation als strafmildernde Faktoren.

Vgl.: 13-stellungnahme-vorstand-thalvenia.md; 18-strategie-vergleichsangebot-bafin.md

Datei: 13-stellungnahme-vorstand-thalvenia.md

13 — Stellungnahme des Vorstands zur BaFin-Anhörung

Adressat: BaFin, Referat VBS 4, z.Hd. Dr. Hannelore Kösters

Absender: Thalvenia Bank AG, vertr. d. d. Vorstand (CEO, COO, CRO)

Verfasser: Schwerbeck Roosendaal mbB im Auftrag der Thalvenia Bank AG

Datum: 28. Juli 2026

Bezug: Az. BaFin VBS 4 1 7-K-22-188/2026; Anhörungsschreiben vom 14. Juli 2026

I. Vorbemerkung

Die Thalvenia Bank AG begrüßt die Möglichkeit zur Stellungnahme und hat das Anhörungsschreiben mit größter Sorgfalt ausgewertet. Der Vorstand nimmt die festgestellten Mängel ernst und hat seit Einleitung der Sonderprüfung im März 2026 umfangreiche Remediation-Maßnahmen ergriffen. Ziel dieser Stellungnahme ist es, zum einen tatsächliche Unrichtigkeiten in den vorläufigen Feststellungen zu korrigieren und zum anderen den Stand der Remediation zu dokumentieren.

II. Zum Cybervorfall Januar 2026 (BAIT Tz. 55)

Vortrag der Thalvenia Bank AG:

Das Institut erkennt an, dass die BaFin-Meldung vom 13. Januar 2026 die Frist des BAIT Tz. 55 nicht einhielt. Es handelte sich jedoch nicht um bewusste Fristversäumnis, sondern um eine Fehlklassifizierung:

1. **Initialer SOC-Alarm (02:17 Uhr, 9. Januar):** Der Schicht-SOC-Mitarbeiter bewertete den SIEM-Alarm aufgrund einer Ähnlichkeit mit einem bekannten Fehlalarm-Muster als False Positive. Diese Entscheidung war menschlich nachvollziehbar, wenn auch im Ergebnis fehlerhaft.

2. **Eskalation (08:30 Uhr, 9. Januar):** Erst mit Entdeckung der verschlüsselten Server und CISO-Benachrichtigung war eine zuverlässige Klassifizierung als wesentlicher IT-Sicherheitsvorfall möglich.

3. **Abwägung:** Der CISO und COO entschieden, vor der BaFin-Meldung zunächst minimale Fakten zu sichern, um eine präzise Erstmeldung zu ermöglichen. Dies entsprach zwar der internen SOC-Handlungsanweisung, nicht aber den BAIT-Anforderungen.

Das Institut hat sämtliche SOC-Prozesse überarbeitet; eine neue interne Anweisung verpflichtet zur sofortigen BaFin-Meldung ab Inkrafttreten der IT-Notfall-Stufe 2, unabhängig vom Informationsstand.

Bitte: Klassifizierung als fahrlässige, nicht vorsätzliche Pflichtverletzung; Berücksichtigung als erstmalige Verfehlung.

III. Zu den AML-/KYC-Mängeln

Vortrag der Thalvenia Bank AG:

Die festgestellten KYC-Lücken werden grundsätzlich eingeräumt. Folgende Entlastungsgesichtspunkte werden vorgetragen:

- **Kunde HR-03 (WiB fehlt):** Das Institut leitete bereits im August 2025 — vor der Sonderprüfung — eine Nacherfüllungsmaßnahme ein, nachdem ein interner AML-Audit die Lücke identifiziert hatte. Die vollständige WiB-Dokumentation lag zum Zeitpunkt der BaFin-Prüfung im April 2026 vor.
- **Kunde HR-07 (Mittelherkunft):** Die dem Institut vorgelegte Mittelherkunftsdocumentation (Stiftungsratserklärung) entsprach dem Marktstandard für Liechtensteiner Stiftungen im Jahr 2020 (Onboarding-Datum). Die verschärften Anforderungen nach § 15 Abs. 4 GwG sind erst durch die GwG-Novelle 2021 konkretisiert worden.
- **PEP-Mängel (HR-11, HR-23, HR-31):** Das Institut war auf die Tier-1-Abdeckung von SymphonyAI angewiesen, die zu den branchenüblichen Standardprodukten zählt. Die BaFin-Auslegungshinweise 2021 verpflichten zu einer risikoadäquaten Datenbankauswahl, die — wie eingeräumt — nicht vollständig umgesetzt wurde. Das Institut hat den Vertrag auf Tier-2-Abdeckung aufgestockt und retrograde PEP-Prüfungen abgeschlossen.

IV. Zu den unterlassenen STR-Meldungen (§ 43 GwG)

Vortrag der Thalvenia Bank AG:

Die fünf im Anhörungsschreiben benannten Transaktionen wurden intern geprüft und die Entscheidung gegen eine Meldung dokumentiert. Die Dokumentation belegt, dass die zuständigen AML-Analysten eine rationale Abwägung vornahmen und zum Ergebnis kamen, dass die Schwelle des § 43 Abs. 1 GwG ("Tatsachen, die darauf hindeuten, dass...") nicht überschritten war. Diese Einschätzung mag im Nachhinein unzutreffend sein; sie war aber zum Entscheidungszeitpunkt vertretbar.

V. Remediation-Stand (Meilensteine)

Maßnahme	Status per 28. Juli 2026
Risikoanalyse § 5 GwG aktualisiert	Abgeschlossen 30. Juni 2026
KYC-Nacherfüllung Hochrisikokunden	Abgeschlossen für HR-03, HR-07, HR-09; HR-19 in Bearbeitung
PEP-Datenbank-Upgrade	Abgeschlossen April 2026
PEP-Retrograde Überprüfung	Abgeschlossen Mai 2026
SOC-Eskalationsprozesse überarbeitet	Abgeschlossen Februar 2026
BAIT-Notfallkonzept überarbeitet	Abgeschlossen Juli 2026
IT-Prüfbericht 2024	Beauftragung April 2026; Bericht erwartet September 2026
AML-Schulung 100 %	Abgeschlossen Juni 2026

VI. Bitte

Der Vorstand der Thalvenia Bank AG bittet die BaFin:

1. Die Anordnung nach § 25a KWG auf die noch ausstehenden Maßnahmen zu beschränken.
2. Beim Bußgeldverfahren die umfangreiche Remediation strafmildernd zu berücksichtigen.
3. Die MiCAR-Entscheidung nicht mit dem Bußgeldverfahren zu verknüpfen, sondern auf Basis des abgeschlossenen Remediationsplans zu treffen.

Bearbeiterin: Prof. Dr. Heinrich Schwertbeck / Dr. Petra Glock-Meinhard

Vgl.: docx/stellungnahme-vorstand-thalvenia-bafin-pruefung.docx

Datei: 14-organisationspflichten-marisk-ba-2024.md

14 — Organisationspflichten MaRisk BA 2024

Rechtsgrundlage: MaRisk BA (BaFin-Rundschreiben 05/2024 (BA) vom 29. Oktober 2024)

Geltungsbereich: Kreditinstitute i.S.d. § 1 Abs. 1 KWG — erfasst Thalvenia Bank AG

Prüfungsrelevanz: AT 4.3 (Aufgaben- und Kompetenzverteilung), AT 7.1 (IT-Strategie), BTO 3 (Handelsgeschäfte)

Überblick relevanter MaRisk-Module

AT 4.3 — Aufgaben- und Kompetenzverteilung

AT 4.3.2 MaRisk verlangt eine klare Aufgaben- und Kompetenzverteilung im Institut, mit eindeutiger Abgrenzung zwischen Front-Office-Aktivitäten und Risikocontrolling. Für die Thalvenia Bank sind folgende Abgrenzungsfragen relevant:

Problematik Eigenhandel Token TN: Die Eigenhandelsaktivitäten in Token TN wurden im Oktober 2024 durch den CEO und COO initiiert, ohne vorherige Genehmigung durch den CRO oder das Risikokomitee. Das interne Regelwerk sah für Kryptowerte-Eigenhandel keine spezifische Zuständigkeit vor. Die CRO (Dr. Birkenhainer) erfuhr von den Aktivitäten erst im Dezember 2024 — nach zwei Monaten aktivem Handel.

Nach AT 4.3.2 MaRisk hätte der Eigenhandel in einem neuen Instrument (Token TN) eine vorherige Produktzulassung durch ein Neues-Produkte-Prozess (NPP) erfordert, der wiederum die Risikofreigabe durch CRO und Risikokomitee voraussetzt.

Befund BaFin: Fehlen eines formellen NPP für Token TN-Eigenhandel; nachträgliche Dokumentation als rückdatierter NPP-Bericht ist nicht akzeptabel.

AT 4.3.3 — Votenpflicht

Nach AT 4.3.3 MaRisk sind für wesentliche Handelsgeschäfte zwei unabhängige Voten erforderlich (Marktseite und Marktfolgeseite). Für den Eigenhandel in Token TN gibt es keine entsprechende Zweivotensystematik. Dies ist aufsichtsrechtlich problematisch, da Kryptowerte trotz ihrer Besonderheiten als Handelsgeschäfte i.S.d. MaRisk behandelt werden.

AT 7.1 — IT-Strategie

AT 7.1 MaRisk verlangt eine mit der Geschäftsstrategie konsistente IT-Strategie. Die IT-Strategie der Thalvenia aus dem Jahr 2022 erwähnt MPC-Technologie und Cold-Custody-Infrastruktur. Der Cybervorfall vom Januar 2026 zeigt jedoch, dass das zugrundeliegende VPN-Gateway seit CVE-2024-21762 (publiziert November 2024) nicht gepatcht worden war — ein Prozessversagen, das auf fehlende Konsistenz zwischen IT-Strategie und Patch-Management hindeutet.

Befund BaFin: IT-Strategie nicht aktuell; kein Nachweis systematischen Schwachstellenmanagements für kritische Infrastrukturkomponenten.

BTO 1.4 / BTO 3 — Handelsgeschäfte

BTO 3 MaRisk (in der Fassung 2024) enthält Anforderungen an Handelsgeschäfte, die analog auf Kryptowerte-Eigenhandel anzuwenden sind. Folgende Anforderungen waren beim Eigenhandel Token TN nicht erfüllt:

Anforderung	Status
Handelslimit für Token TN	Nicht vorhanden
Stop-Loss-Regelung	Nicht vorhanden
Bewertungsmodell für illiquide Token	Marktwert-Bewertung, aber kein Modell für Marktliquidität
Interday-Positionsüberwachung	Nicht täglich durch CRO
Dokumentation Handelsstrategien	Nur informell

Auswirkungen auf das MiCAR-Verfahren

Die MaRisk-Mängel haben unmittelbare Relevanz für das MiCAR-CASP-Verfahren. Art. 68 MiCAR stellt an CASPs governance-bezogene Anforderungen, die inhaltlich mit MaRisk übereinstimmen. Wenn die BaFin MaRisk-Verstöße als Beleg für eine unzureichende interne Governance wertet, gefährdet dies den CASP-Antrag.

Remediationsmaßnahmen

Das Institut hat nach Mandatserteilung an Schwertbeck Roosendaal folgende Maßnahmen zur MaRisk-Compliance ergriffen:

1. Nachträglicher NPP-Prozess für Token TN-Eigenhandel; CRO-Freigabe und Risikokomitee-Beschluss nachgeholt (April 2026).
2. Eigenhandels-Limits für Token TN: Positionslimit EUR 10 Mio., Stop-Loss bei -15 %, Daily P&L-Reporting an CRO.
3. IT-Strategie überarbeitet: Schwachstellenmanagement-Prozess formalisiert; SLA für kritische Patches: 72 Stunden nach CVE-Veröffentlichung.
4. BTO-3-konformes Zweivoten-System für Kryptowerte-Eigenhandel implementiert.

Quellen: bafin.de, MaRisk BA 2024, Rundschreiben 05/2024 (BA); bundesgerichtshof.de zu Bankorganisationspflichten BGH XI ZR 372/09.

Datei: 15-zustaendigkeitsabgrenzung-bafin-fiu-bnetza.md

15 — Zuständigkeitsabgrenzung BaFin / FIU / BNetzA

Dokument: Interne Kanzleinotiz zur Behördenkoordination

Datum: 5. April 2026

Bearbeiterin: Dr. Petra Glock-Meinhard

Ausgangslage: Drei parallele Behördenverfahren

Die Thalvenia Bank AG ist gleichzeitig Gegenstand von Verfahren bei drei verschiedenen Behörden:

1. **BaFin** (Bonn/Frankfurt): Sonderprüfung VBS 4 1 7-K-22-188/2026 (Bankaufsicht, AML-Aufsicht, Marktintegrität)
2. **FIU** (Köln): Auskunftersuchen 2026-FIU-7711-TN (Geldwäscheanalyse)
3. **BNetzA** (Bonn): Schreiben vom 3. April 2026 zur Cybersicherheitsmeldepflicht nach BSIG

Dazu kommt die **Staatsanwaltschaft Stuttgart** (Strafverfahren gegen CCO), die jedoch formal eine andere Rechtsmaterie betrifft.

Zuständigkeit BaFin

Die BaFin ist als Allfinanzaufsicht nach KWG, GwG, WpHG/MiCAR und BAIT für die prudenzielle und verhaltensbezogene Aufsicht über das Institut zuständig. Ihre Befugnisse umfassen:

- Sonderprüfungen nach § 44 KWG

- Anordnungen nach § 25a KWG
- Bußgeldverfahren nach § 56 GwG, § 60b GwG
- Untersagung nach § 6 Abs. 3 KWG
- Widerruf der Zulassung nach § 35 KWG
- CASP-Zulassung / -Versagung nach Art. 63 MiCAR

Die BaFin koordiniert mit der FIU gemäß § 29 Abs. 1 GwG (gegenseitige Informationspflicht BaFin-FIU) und mit der Staatsanwaltschaft gemäß § 4 Abs. 5 GwG (Übermittlungspflicht bei Geldwäscheverdacht).

Zuständigkeit FIU

Die FIU (§ 27 GwG) ist als Zentralstelle für Finanztransaktionsuntersuchungen organisatorisch beim Zoll (Bundeszollamt) angesiedelt. Ihre Befugnisse beschränken sich auf:

- Entgegennahme von Verdachtsmeldungen nach § 43 GwG
- Analyse und ggf. Weiterleitung an Strafverfolgungsbehörden (§ 32 GwG)
- Auskunftersuchen an Institute (§ 30 GwG)
- Einfrierungsanordnungen in Ausnahmefällen

Die FIU hat **keine** direkte Sanktionsbefugnis gegenüber dem Institut. Sie kann jedoch Informationen an die BaFin übermitteln, die dann sanktioniert. Das Auskunftersuchen der FIU vom 22. Februar 2026 ist daher primär ein Informationsgathering, das in den BaFin-Bußgeldrahmen einfließen kann.

Tipping-off-Verbot (§ 44 GwG): Das Institut darf die betroffenen Kunden (HR-07, HR-11) nicht über das FIU-Auskunftersuchen informieren. Dies gilt auch für die Anwälte der betroffenen Kunden, sofern sie nicht Verteidiger im FIU-Verfahren sind.

Zuständigkeit BNetzA

Die Bundesnetzagentur ist nach § 8a BSIG (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik) für kritische Infrastrukturen zuständig. Das Schreiben vom 3. April 2026 fragt an, ob die Thalvenia Bank AG als Betreiber kritischer Infrastrukturen im Sektor Finanzen einzustufen ist.

Rechtslage:

- Kreditinstitute mit Bilanzsumme über EUR 30 Mrd. sind KRITIS-Betreiber (§ 2 Abs. 10 BSIG i.V.m. BSI-KritisV).
- Thalvenia (Bilanzsumme ca. EUR 700 Mio.) liegt erheblich unter diesem Schwellenwert.
- **Ergebnis:** Thalvenia ist kein KRITIS-Betreiber; eine BSIG-Meldepflicht nach § 8b BSIG besteht nicht.

Dennoch besteht nach dem NIS2-Umsetzungsgesetz (in Kraft seit Oktober 2024) eine Meldepflicht für "wichtige Einrichtungen" im Finanzsektor bei erheblichen Sicherheitsvorfällen an das BSI. Diese Pflicht ist von der BAIT-Meldepflicht gegenüber der BaFin zu unterscheiden.

Empfehlung: BNetzA-Anfrage beantworten mit Verweis auf fehlende KRITIS-Eigenschaft; gleichzeitig prüfen, ob NIS2-Meldepflicht (BSI) neben der BAIT-Meldepflicht (BaFin) ausgelöst wurde.

Koordinationsstrategie

Um Widersprüche in den parallelen Verfahren zu vermeiden, hat die Kanzlei folgende Koordinationsregeln aufgestellt:

1. **Einheitliche Sachverhaltsdarstellung:** Alle Behördenschreiben und -antworten werden von der Kanzlei koordiniert; keine abweichenden Darstellungen.
2. **Informationsprimat BaFin:** BaFin als primäre Aufsichtsbehörde hat Priorität; FIU-Antworten orientieren sich an der BaFin-Darstellung.
3. **Trennungsgebot Strafrecht:** Die Antworten an BaFin und FIU berücksichtigen das Strafverfahren gegen Dr. Tannenfels; selbstbelastende Angaben zu seinen Handlungen werden vermieden.
4. **Dokumentation aller Behördenkontakte:** Vollständiges Protokoll aller Telefonate, Schreiben und E-Mails mit allen drei Behörden.

Vgl.: 16-individual-strafverfahren-vorstand.md; 10-suspicious-transaction-reports-fiu.md

Datei: 16-individual-strafverfahren-vorstand.md

16 — Individual-Strafverfahren gegen den Vorstand

Beschuldigter: Dr. Lasse Tannenfels (CCO der Thalvenia Bank AG)

Staatsanwaltschaft: Stuttgart, Az. 13 Js 4481/26

Tatvorwurf: Verdacht der Geldwäsche (§ 261 StGB)

Ermittlungsbeginn: Februar 2026

Strafverteidigerin: RAin Dr. Franziska Oberkampf-Heyden, Frankfurt (getrennt mandatiert)

Sachverhalt nach Aktenlage

Die Staatsanwaltschaft Stuttgart ermittelt gegen Dr. Tannenfels aufgrund eines anonymen Hinweises, der im Dezember 2025 bei der FIU und anschließend bei der Staatsanwaltschaft einging. Der Hinweis behauptete, Dr. Tannenfels habe gewusst, dass Transaktionen des Kunden HR-07 aus krimineller Vortat (mutmaßlich Bestechung im Ausland, § 334 StGB) herrührten, diese Transaktionen aber nicht der FIU gemeldet.

Tatbestand § 261 StGB

§ 261 StGB (Geldwäsche) setzt in der aktuellen Fassung (seit GwG-Novelle 2021 "All-Crime-Ansatz") voraus:

- Einen Vermögensgegenstand, der aus einer rechtswidrigen Tat herrührt (Vortatunabhängigkeit: alle rechtswidrigen Taten qualifizieren als Vortat)
- Verbergen, Verschleiern, Ermöglichen des Verdeckens oder Nichtmelden trotz gesetzlicher Pflicht (§ 261 Abs. 1 S. 1 StGB)

Der Vorwurf gegen Dr. Tannenfels lautet konkret: Er habe als Geldwäschebeauftragter Kenntnis von der möglichen kriminellen Herkunft von Geldern des HR-07 gehabt (aufgrund interner Analyse-Vermerke), die Meldung nach § 43 GwG aber pflichtwidrig unterlassen und damit das Verbergen der Herkunft ermöglicht.

§ 54a KWG — Strafbarkeit von Bankvorständen

Zusätzlich prüft die Staatsanwaltschaft eine mögliche Strafbarkeit nach § 54a KWG (Gefährdung der Solidität des Instituts). § 54a Abs. 1 KWG stellt unter Strafe, wer entgegen einer vollziehbaren Anordnung der BaFin handelt. Da die BaFin noch keine Anordnung erlassen hat, scheidet § 54a KWG derzeit aus. Sollte die BaFin nach dem Abschluss der Sonderprüfung eine Anordnung nach § 25a KWG erlassen und das Institut dieser nicht nachkommen, könnte § 54a KWG relevant werden.

Interessenkonflikt und Trennungsgebot

Der Interessenkonflikt zwischen Dr. Tannenfels als Beschuldigtem und dem Institut ist erheblich:

- Als CCO ist Dr. Tannenfels noch im Amt (Stand Juli 2026). Der Aufsichtsrat hat noch keine Abberufung beschlossen.
- Das Institut hat ein Eigeninteresse daran, gegenüber der BaFin zu betonen, dass AML-Entscheidungen nach einem ordnungsgemäßen Prozess getroffen wurden.
- Dr. Tannenfels hat als Beschuldigter ein Schweigerecht (§ 136 StPO).
- Jede Aussage des Instituts gegenüber der BaFin, die auf interne Analysen des CCO abstellt, könnte strafprozessual gegen Dr. Tannenfels verwendet werden.

Konsequenz: Schwertbeck Roosendaal und RAin Dr. Oberkampf-Heyden haben vereinbart, dass alle Aussagen des Instituts gegenüber der BaFin, die sich auf Handlungen von Dr. Tannenfels beziehen, mit Dr. Oberkampf-Heyden abgestimmt werden. Dr. Tannenfels wird in der Stellungnahme an die BaFin nicht namentlich als Verantwortlicher für konkrete AML-Entscheidungen benannt.

Aufsichtsrechtliche Parallelprüfung: § 33 KWG — Eignung

Unabhängig vom Strafverfahren kann die BaFin nach § 33 Abs. 1 S. 1 Nr. 2 KWG die Zuverlässigkeit des CCO neu bewerten, wenn Tatsachen bekannt werden, die eine Unzuverlässigkeit begründen. Ein laufendes Ermittlungsverfahren begründet noch keine Unzuverlässigkeit, kann aber die BaFin zu einer Befragung veranlassen.

Der Aufsichtsrat hat sich darauf verständigt, Dr. Tannenfels bis zum Abschluss des Strafverfahrens im Amt zu belassen, aber seine operativen Befugnisse auf das Notwendige zu beschränken; die FIU-Kommunikation ist auf Dr. Glock-Meinhard (externe Kanzlei) und Dr. Miriam Hoffrath-Seel (Leiterin Rechtsabteilung) übertragen worden.

Risikobewertung

Die Kanzlei bewertet das Strafverfahren als ernstzunehmendes, aber beherrschbares Risiko. Kernfrage ist, ob die Staatsanwaltschaft nachweisen kann, dass Dr. Tannenfels positive Kenntnis von der kriminellen Herkunft der HR-07-Gelder hatte. Die Akte zeigt bislang interne Vermerke, die Zweifel an der Mittelherkunft dokumentieren, aber keine definitiv-positive Kenntnis belegen.

Vgl.: 10-suspicious-transaction-reports-fiu.md; 15-zustaendigkeitsabgrenzung-bafin-fiu-bnetza.md

Datei: 17-sanktionsrahmen-bussgeld-untersagung.md

17 — Sanktionsrahmen: Bußgeld und Untersagung

Dokument: Rechtliche Analyse Sanktionsrisiken

Kanzlei: Schwertbeck Roosendaal mbB

Datum: 1. Juli 2026

Bearbeiterin: Dr. Petra Glock-Meinhard

Bußgeldrahmen nach GwG

§ 56 GwG (Ordnungswidrigkeiten)

§ 56 GwG normiert den bußgeldrechtlichen Rahmen für Verstöße gegen die Pflichten des GwG. Für juristische Personen (hier: Thalvenia Bank AG) gelten folgende Obergrenzen:

Verstoß	Bußgeldrahmen	Anwendbare Norm
Verletzung der Sorgfaltspflichten (§§ 10-14 GwG)	Bis zu EUR 5 Mio. oder 10 % Jahresumsatz	§ 56 Abs. 1 Nr. 63 GwG
Verletzung der verstärkten Sorgfaltspflichten (§ 15 GwG)	Bis zu EUR 5 Mio. oder 10 % Jahresumsatz	§ 56 Abs. 1 Nr. 67 GwG
Unterlassene Verdachtsmeldung (§ 43 GwG)	Bis zu EUR 5 Mio. oder 10 % Jahresumsatz	§ 56 Abs. 1 Nr. 70 GwG
Verletzung der Organisationspflichten (§ 6 GwG)	Bis zu EUR 1 Mio.	§ 56 Abs. 1 Nr. 53 GwG

Für besonders schwere und systematische Verstöße nach § 56 Abs. 2 GwG erhöht sich die Obergrenze auf EUR 5 Mio. oder alternativ 10 % des Gesamtumsatzes. Der Jahresumsatz der Thalvenia Bank AG beträgt ca. EUR 62 Mio.; 10 % entsprächen EUR 6,2 Mio.

Kanzlei-Schätzung Bußgeldhöhe: Bei Berücksichtigung der ergriffenen Remediation-Maßnahmen, der erstmaligen Verfehlung und der kooperativen Haltung: EUR 1,2 Mio. bis EUR 2,8 Mio. Ohne Settlement-Einigung und bei Verschlechterung der Kooperationshaltung: bis zu EUR 4,5 Mio.

§ 60b GwG (Veröffentlichung)

§ 60b GwG verpflichtet die BaFin zur Veröffentlichung rechtskräftiger Bußgeldbescheide für Kreditinstitute im Internet. Die Veröffentlichung erfolgt mit Name des Instituts, Art des Verstoßes und Höhe des Bußgelds und verbleibt für fünf Jahre online.

Reputationsrisiko: Eine öffentliche Veröffentlichung nach § 60b GwG würde erhebliche Reputationsschäden für die Thalvenia Bank AG verursachen, insbesondere gegenüber institutionellen Kunden, die interne AML-Compliance-Standards einhalten müssen. Das Institut muss im Rahmen der Settlement-Strategie (vgl. 18-strategie-vergleichsangebot-bafin.md) versuchen, eine nicht-öffentliche Einigung zu erzielen.

Aufsichtsrechtliche Maßnahmen nach KWG

§ 6 Abs. 3 KWG — Untersagung des Geschäftsbetriebs

Die BaFin kann nach § 6 Abs. 3 KWG den Betrieb eines Kreditinstituts ganz oder teilweise untersagen, wenn der ordnungsgemäße Geschäftsbetrieb gefährdet ist. Dies ist die schärfste Maßnahme unterhalb des Lizenzentzugs und kann als sofortige Unterbindung spezifischer Aktivitäten (z.B. Eigenhandel Token TN) oder als vollständige Untersagung ausgesprochen werden.

Einschätzung: Eine vollständige Untersagung ist unwahrscheinlich, da das Institut seine Cold-Custody-Kerndienstleistung aufrecht hält und die Kundenvermögen zu keiner Zeit gefährdet waren. Eine partielle Untersagung des Eigenhandels in Token TN ist realistisch als Settlement-Vereinbarung.

§ 35 Abs. 2 KWG — Widerruf der Zulassung

Ein Lizenzentzug nach § 35 Abs. 2 KWG kommt in Betracht, wenn das Institut nachhaltig aufsichtsrechtliche Anforderungen verletzt oder der Geschäftsbetrieb gravierend gefährdet ist. Diese Schwelle ist nach dem aktuellen Sachstand nicht erreicht. Das Institut wäre in einem solchen Fall wirtschaftlich nicht lebensfähig (EUR 4,3 Mrd. AuM wären zu übertragen); die BaFin würde dies als ultima ratio einsetzen.

BAIT-Sanktionen

Für den Cybervorfall-Meldungsverzug ist kein spezifischer GwG-Tatbestand einschlägig. Die BAIT begründet keine eigenständige Bußgeldbewehrung; stattdessen fließt der BAIT-Verstoß in die Beurteilung nach § 25a KWG ein. Eine Anordnung nach § 25a KWG ist kein Sanktionsinstrument, sondern eine Verpflichtung zur Mängelbeseitigung.

Strafrecht — Individuelle Sanktionen

Für individuelle Verstöße (Dr. Tannenfels, § 261 StGB) gelten die allgemeinen strafrechtlichen Sanktionsnormen: Freiheitsstrafe bis zu 5 Jahren oder Geldstrafe. Bei minder schweren Fällen (§ 261 Abs. 4 StGB) bis zu 2 Jahre oder Geldstrafe. Die Staatsanwaltschaft Stuttgart prüft derzeit noch, ob hinreichender Tatverdacht vorliegt.

Vgl.: 18-strategie-vergleichsangebot-bafin.md

Datei: 18-strategie-vergleichsangebot-bafin.md

18 — Vergleichsstrategie und Settlement-Angebot an die BaFin

Dokument: Strategiepapier für Settlement-Verhandlung

Kanzlei: Schwertbeck Roosendaal mbB

Datum: 20. Juli 2026

Bearbeiterin: Prof. Dr. Heinrich Schwertbeck

Vorbemerkung

Die BaFin führt im deutschen Aufsichtsrecht kein formelles "Settlement"-Verfahren wie etwa die SEC in den USA. Es gibt jedoch eine gewachsene Praxis, bei der Instituten vor dem Erlass eines Bußgeldbescheids Gelegenheit gegeben wird, Abhilfemaßnahmen als Undertakings zuzusagen und

dadurch die Bußgeldhöhe und -öffentlichkeit zu beeinflussen. Diese Praxis wird in der Anhörungsphase nach § 28 VwVfG realisiert.

Settlement-Strategie

Strategie-Elemente

Element 1 — Kooperation als Hauptargument Das Institut kooperiert seit Einleitung der Prüfung vollständig. Es hat alle angeforderten Dokumente vollständig und fristgerecht geliefert. Es hat keine Verfahrenshindernisse errichtet. Diese Haltung soll explizit als strafmildernder Umstand vorgetragen werden.

Element 2 — Undertakings zur Remediation Das Institut bietet folgende verbindliche Undertakings an:

- Vorlage des IT-Prüfberichts 2024 innerhalb von 45 Tagen nach BaFin-Bescheid
- Vollständige KYC-Nacherfüllung für alle Hochrisikokunden bis 30. September 2026
- Einstellung des Token-TN-Eigenhandels bis zur BaFin-Freigabe (faktische Eigentätigkeit eingestellt ab August 2026)
- Externe AML-Prüfung durch einen von der BaFin akzeptierten Wirtschaftsprüfer (KPMG) bis 31. Oktober 2026

Element 3 — Bußgeldhöhe Das Institut bietet an, einem Bußgeld in Höhe von EUR 1,5 Mio. zuzustimmen, wenn die BaFin auf eine Veröffentlichung nach § 60b GwG verzichtet oder diese auf eine Minifassung ohne institutsspezifische Details reduziert. Eine Veröffentlichung ohne Namensnennung ist nach § 60b Abs. 5 GwG möglich, wenn die Veröffentlichung verhältnismäßig wäre oder persönliche Daten schützt — hier analog der Institutspersönlichkeit.

Element 4 — MiCAR-Verbindung Das Institut bittet, den CASP-Zulassungsantrag von den Bußgeldüberlegungen zu trennen. Konkret wird angeboten:

- Wenn die BaFin den CASP-Antrag positiv bescheidet, wird das Institut eine zusätzliche freiwillige Zahlung von EUR 200.000 für ein BaFin-Fortbildungsprogramm leisten (kein Bußgeld, sondern freiwillige Unterstützungsmaßnahme).
- Das Institut stimmt einer jährlichen Sonderprüfung durch BaFin für die ersten drei Jahre nach CASP-Zulassung zu.

Vergleichskorridor

Szenario	Bußgeld (Institute)	Veröffentlichung	MiCAR	Eigenhandel Token TN
Best Case (Settlement einig)	EUR 1,5 Mio.	Keine Namensnennung	CASP erteilt Q3 2026	Eingestellt bis Freigabe
Mid Case (teilweise Einigung)	EUR 2,5 Mio.	Kurzmeldung	CASP erteilt Q4 2026	Eingestellt auf unbestimmte Zeit
Worst Case (kein Settlement)	EUR 4,0-5,0 Mio.	Vollständige Veröffentlichung	CASP gefährdet/ versagt	Mögliche partielle Untersagung

Verfahrensablauf Settlement-Verhandlung

1. **28. Juli 2026:** Einreichung formelle Stellungnahme mit Undertakings (vgl. 13-stellungnahme-vorstand-thalvenia.md)
2. **August 2026:** Bilateral-Gespräch Dr. Kösters / Prof. Dr. Schwertbeck zur Diskussion Settlement-Optionen
3. **September 2026:** Formelles Settlement-Angebot in Briefform an BaFin-Präsidentin
4. **Oktober 2026:** BaFin-Entscheidung (Bußgeldbescheid oder Verfahrenseinstellung bei Settlement)

MAR-Verfahren (Token TN)

Für den noch in der Voruntersuchung befindlichen MAR-Sachverhalt empfiehlt die Kanzlei, aktiv auf eine Voruntersuchungs-Einstellung hinzuwirken. Argumente:

- Kein Nachweis koordinierter Handlungen mit HR-07
- Institut hat Token-TN-Eigenhandel eingestellt (Remediation)
- Die fraglichen Kurseffekte könnten auch auf breite Marktbewegungen zurückzuführen sein

Die Kanzlei wird ein externes Sachverständigengutachten zu den Kurseffekten in Auftrag geben.

Vgl.: 17-sanktionsrahmen-bussgeld-untersagung.md; 21-roadmap-remediation-100-tage.md

Datei: 19-pressemitteilung-entwurf.md

19 — Pressemitteilung (Entwurf)

Status: Entwurf — nicht veröffentlicht

Datum Entwurf: 2. August 2026

Autorin: Dr. Petra Glock-Meinhard / IR-Team Thalvenia

Freigabe erforderlich durch: Vorstand, Aufsichtsrat, Kanzlei Schwertbeck Roosendaal

Hinweis: Freigabe steht aus; Veröffentlichungszeitpunkt abhängig von BaFin-Entscheid

ENTWURF — FÜR INTERNE ABSTIMMUNG — NICHT ZUR VERÖFFENTLICHUNG

Pressemitteilung

Thalvenia Bank AG Stuttgart

Stuttgart, [Datum einfügen] — Thalvenia Bank AG kommentiert laufende BaFin-Prüfung und kommuniziert Maßnahmen zur Compliance-Stärkung

Die Thalvenia Bank AG (Thalvenia), eines der führenden deutschen Spezialinstitute für institutionelle Kryptoverwahrung, gibt im Zusammenhang mit der im März 2026 eingeleiteten Sonderprüfung durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) folgende Erklärung ab:

Über die BaFin-Prüfung

Im Rahmen der regulären Aufsichtstätigkeit der BaFin wurde die Thalvenia Bank AG einer Sonderprüfung nach § 44 KWG unterzogen. Diese Prüfung hat Bereiche identifiziert, in denen das Institut seine internen

Prozesse und Dokumentation verbessern kann. Thalvenia nimmt die regulatorischen Anforderungen ernst und hat aktiv mit der BaFin kooperiert.

Maßnahmen

Thalvenia hat seit März 2026 ein umfassendes Programm zur Stärkung seiner Compliance-Strukturen eingeleitet, das folgende Bereiche umfasst:

- Aktualisierung der Geldwäsche-Risikoanalyse und Verstärkung der Kundensorgfaltsprozesse
- Upgrade des PEP-Screening-Systems auf erweiterte Datenbankabdeckung
- Überarbeitung der IT-Sicherheitsprozesse, einschließlich SOC-Eskalationsverfahren und Notfallkonzepte
- Einführung eines neuen Produkt-Genehmigungsprozesses für alle neuen Handelsinstrumente
- Erhöhung der Schulungsquote für AML-relevante Mitarbeiter auf 100 %

"Wir nehmen regulatorische Anforderungen sehr ernst", erklärt CEO Dr. Cornelius Thalheim-Lattermann. "Die identifizierten Verbesserungsbedarfe haben wir umgehend adressiert. Unsere Kunden können sich auf die Sicherheit ihrer Vermögen und die Integrität unserer Prozesse verlassen."

MiCAR-Zulassung

Thalvenia beantragte im November 2024 die Zulassung als Crypto-Asset Service Provider (CASP) nach der europäischen MiCAR-Verordnung. Das Verfahren läuft regulär und das Institut ist zuversichtlich, die Zulassung zu erhalten.

Kundenvermögen

Die verwalteten Kundenvermögen in Höhe von EUR 4,3 Mrd. waren zu keinem Zeitpunkt gefährdet. Die Kerndienste des Instituts — Cold Custody, MPC Signing und Staking Services — waren mit Ausnahme eines kurzen, nicht kundenrelevanten Serviceausfalls im Januar 2026 durchgehend verfügbar.

Über Thalvenia Bank AG

Die Thalvenia Bank AG ist ein Stuttgarter Spezialinstitut für institutionelle Kryptoverwahrung. Mit einer Zulassung seit Oktober 2020 ist Thalvenia eines der pionierenden deutschen Kryptoverwahrungsinstitute. Das Institut verwaltet Kryptovermögen für institutionelle Anleger in Deutschland, der Schweiz und Österreich.

Interne Kommentare zur Entwurfsfassung

Prof. Dr. Schwertbeck (27.07.2026, mündlich): "Die Formulierung zur BaFin-Prüfung ist zu vage. Es muss deutlich werden, dass es sich um eine reguläre Sonderprüfung ohne Lizenzzug-Risiko handelt. Außerdem: Bitte das MAR-Verfahren Token TN nicht erwähnen — das ist noch in der Voruntersuchungsphase."

CRO Dr. Birkenhainer (28.07.2026, E-Mail): "CEO-Zitat ist gut. Bitte aber keinen Verweis auf 'Verbesserungsbedarfe' — das klingt defensiv. Besser: 'proaktive Compliance-Initiative'."

Aufsichtsratsvorsitzender Klaus-Dieter Henfling (mündlich, 01.08.2026): "Pressemitteilung nicht herausgeben, bis BaFin-Entscheid feststeht. Wir müssen die Botschaft kontrollieren."

Empfehlung Kanzlei: Pressemitteilung erst nach finalem BaFin-Bescheid und nach Abstimmung mit § 60b GwG-Veröffentlichung (falls zutreffend) herausgeben. Im Best-Case-Settlement-Szenario kann die PM zusammen mit der BaFin-Einigung veröffentlicht werden und so die Botschaft aktiv steuern.

Datei: 20-aufsichtsratsbericht.md

20 — Bericht an den Aufsichtsrat

Adressat: Aufsichtsrat der Thalvenia Bank AG

Verfasser: Vorstand der Thalvenia Bank AG (CEO Dr. Thalheim-Lattermann, COO Vellbruck, CRO Dr. Birkenhainer)

Kanzleibegleitung: Prof. Dr. Heinrich Schwertbeck

Datum: 1. August 2026

Anlass: Außerordentliche AR-Sitzung 5. August 2026

I. Zusammenfassung für den Aufsichtsrat

Der Vorstand informiert den Aufsichtsrat über den Stand der BaFin-Sonderprüfung VBS 4 1 7-K-22-188/2026, das FIU-Verfahren 2026-FIU-7711-TN, das Strafverfahren gegen CCO Dr. Tannenfels und die MiCAR-Übergangslizenz. Die Gesamtlage ist ernst, aber beherrschbar. Das Institut hat umfangreiche Remediation-Maßnahmen ergriffen; die Kerndienstleistungen sind nicht unterbrochen.

II. Pflichten des Aufsichtsrats nach § 25d KWG und § 90 AktG

§ 25d KWG — Aufsichtsrat und Risikoausschuss

§ 25d KWG stellt besondere Anforderungen an die Qualifikation von Aufsichtsratsmitgliedern bei Kreditinstituten und verpflichtet zur Einrichtung eines Risikoausschusses (§ 25d Abs. 8 KWG). Der Risikoausschuss der Thalvenia Bank AG besteht aus:

- Klaus-Dieter Henfling (AR-Vorsitzender, Bankkaufmann mit Erfahrung im Retail-Banking)
- Prof. Dr. Elke Strauch-Metzner (Professorin für Bankrecht, Uni Mainz)
- Dietmar Kohlfurter (ehemaliger Leiter IT-Sicherheit eines DAX-Unternehmens)

§ 90 AktG — Berichtspflichten des Vorstands

Der Vorstand ist nach § 90 Abs. 1 Nr. 4 AktG verpflichtet, dem Aufsichtsrat über Geschäfte zu berichten, die für die Rentabilität oder Liquidität der Gesellschaft von erheblicher Bedeutung sein können. Die BaFin-Prüfung mit möglichem Bußgeld bis zu EUR 5 Mio. und das Risiko des MiCAR-Zulassungsversagens sind solche Geschäfte.

III. Aktuelle Lage (Stand 1. August 2026)

A. BaFin-Sonderprüfung

Aspekt	Status
Prüfung abgeschlossen	Ja (30. Juni 2026)
Anhörungsschreiben	14. Juli 2026 erhalten
Stellungnahme eingereicht	28. Juli 2026
Mögliches Bußgeld	EUR 1,5 Mio. bis EUR 5 Mio.
Mögliche § 25a KWG-Anordnung	Wahrscheinlich; Umfang begrenzt

B. MiCAR-Zulassung

Aspekt	Status
Antrag eingereicht	14. November 2024
Vollständigkeitsbescheinigung	20. Januar 2025
Erwartete Entscheidung	Q4 2026 (nach BaFin-Bescheid)
Risiko Versagung	Mittel (bei gutem Settlement: niedrig)

C. FIU-Verfahren

Aspekt	Status
Auskunftersuchen beantwortet	15. März 2026
Laufende FIU-Analyse	Unbekannt
Risiko Strafanzeige an StA	Mittel

D. Strafverfahren Dr. Tannenfels

Aspekt	Status
Ermittlungsverfahren	Eingeleitet Februar 2026
Getrennte Strafverteidigung	Dr. Oberkampf-Heyden
Amt-/Abberufungsfrage	AR-Entscheidung ausstehend

IV. D&O-Risiko

Der Aufsichtsrat muss prüfen, ob Vorstandsmitglieder persönliche Haftungsrisiken aus der Sonderprüfung tragen. Die D&O-Versicherung (Versicherungssumme EUR 50 Mio.) wurde durch Willis Towers Watson zur Prüfung übermittelt. Erste Einschätzung des Versicherers: AML-Versäumnisse sind grundsätzlich nicht vom D&O-Ausschluss für wissentliche Pflichtverletzungen erfasst, solange kein Vorsatz nachgewiesen ist.

V. Empfehlung des Vorstands an den Aufsichtsrat

1. Ermächtigung zur Führung von Settlement-Verhandlungen mit der BaFin.
2. Beschluss über Beauftragung KPMG als externe AML-Prüferin.
3. Erörterung der Abberufungsfrage CCO Dr. Tannenfels.
4. Kenntnisnahme der Remediation-Roadmap (100 Tage).
5. Freigabe der Pressemitteilung nach BaFin-Entscheid.

Vgl.: 21-roadmap-remediation-100-tage.md; 18-strategie-vergleichsangebot-bafin.md

21 — Remediation-Roadmap: 100-Tage-Plan

Planungsbeginn: 1. August 2026

Planungsende (100 Tage): 9. November 2026

Verantwortlich: CRO Dr. Annegret Birkenhainer (Overall Lead), CCO Dr. Tannenfels (soweit im Amt)

Kanzleibegleitung: Schwertbeck Roosendaal mbB

Koordination extern: KPMG AG (AML-Prüfung ab September 2026)

Überblick: Meilensteine

Meilenstein	Frist	Verantwortlich	Status
M1: AML-Sofortmaßnahmen abgeschlossen	31. August 2026	CCO / Legal	In Bearbeitung
M2: IT-Prüfbericht 2024 vorgelegt	15. September 2026	CTO Magnus Thorvaldsson	Beauftragung abgeschlossen
M3: KPMG-Erstbericht AML-Prüfung	31. Oktober 2026	KPMG / CRO	Beauftragung abgeschlossen
M4: MiCAR-Compliance vollständig	31. Oktober 2026	CCO / Legal	In Planung
M5: Settlement-Einigung BaFin	Oktober 2026	Kanzlei / CEO	Verhandlungen Oktober 2026
M6: Abschlussbericht Remediation	9. November 2026	CRO / Kanzlei	Ausstehend

Detailplan nach Themenbereichen

Bereich 1: AML / GwG

Aufgabe	Frist	Status
Risikoanalyse § 5 GwG aktualisiert und genehmigt	Abgeschlossen 30.06.2026	Abgeschlossen
KYC-Nacherfüllung HR-03, HR-07, HR-09	Abgeschlossen 30.06.2026	Abgeschlossen
KYC-Nacherfüllung HR-11, HR-19	31.08.2026	In Bearbeitung
PEP-Datenbank SymphonyAI Tier 2	Abgeschlossen April 2026	Abgeschlossen

Aufgabe	Frist	Status
Retrograde PEP-Überprüfung (alle HR-Kunden)	Abgeschlossen Mai 2026	Abgeschlossen
AML-Schulung 100 % Abdeckung	Abgeschlossen Juni 2026	Abgeschlossen
Überarbeitung Monitoring-Regelwerk	31.08.2026	In Bearbeitung
Vertretungsregelung Geldwäschebeauftragter	15.08.2026	Offen
AML-Handbuch v3.4 verabschiedet	30.09.2026	Geplant
KPMG externe Prüfung abgeschlossen	31.10.2026	Geplant

Bereich 2: IT-Sicherheit / BAIT

Aufgabe	Frist	Status
FortiGate VPN-Patch (Notfallpatch)	Abgeschlossen 10.01.2026	Abgeschlossen
SOC-Eskalationsprozesse überarbeitet	Abgeschlossen Februar 2026	Abgeschlossen
BAIT-Notfallkonzept überarbeitet	Abgeschlossen Juli 2026	Abgeschlossen
IT-Prüfbericht 2024 vorgelegt	15.09.2026	In Beauftragung
BCM-Test MPC-Signing-System	30.09.2026	Geplant
Schwachstellen-SLA (72h Patch) formalisiert	Abgeschlossen Juli 2026	Abgeschlossen

Bereich 3: MaRisk / Governance

Aufgabe	Frist	Status
NPP-Prozess Token TN nachgeholt	Abgeschlossen April 2026	Abgeschlossen
Eigenhandels-Limits Token TN definiert	Abgeschlossen April 2026	Abgeschlossen
Token TN Eigenhandel eingestellt	Abgeschlossen August 2026	Abgeschlossen
Zweivoten-System Kryptowerte-Handel	Abgeschlossen Juli 2026	Abgeschlossen
Interessenkonflikt-Policy MiCAR Art. 72	31.08.2026	In Bearbeitung

Bereich 4: MiCAR-Compliance

Aufgabe	Frist	Status
White Papers Token-Kategorien (3 ausstehend)	30.09.2026	Geplant
TFR-Compliance Travel Rule	31.10.2026	Geplant
MiCAR Art. 68 Governa nce-Dokumentation	31.10.2026	Geplant

KPI-Matrix

KPI	Ziel	Aktuell	Trend
KYC-Vollständigkeit Hochrisikokunden	100 %	75 %	Steigend
PEP-Screening-Abdeck ung Tier 2	100 %	100 %	Erfüllt
AML-Schulungsquote	100 %	100 %	Erfüllt
Offene kritische BAIT-Findings	0	2	Sinkend
Monitoring-Regelwerk- Aktualität	Aktuell	Veraltet	In Bearbeitung

Vgl.: 22-abschlussvermerk-anwalt.md

Datei: 22-abschlussvermerk-anwalt.md

22 — Anwaltlicher Abschlussvermerk

Kanzlei: Schwertbeck Roosendaal mbB, Frankfurt am Main

Aktenzeichen: SR-2026-FIN-0612

Vermerk-Datum: 10. August 2026

Verfasser: Prof. Dr. Heinrich Schwertbeck

Status: Zwischenvermerk (finaler Abschluss nach BaFin-Entscheid)

I. Sachverhaltsübersicht

Die Thalvenia Bank AG, Kryptoverwahrungsunternehmen mit MiCAR-Übergangstatus, war Gegenstand einer BaFin-Sonderprüfung (Az. VBS 4 1 7-K-22-188/2026), die zwischen April und Juni 2026 in Stuttgart stattfand. Die Prüfung hat schwerwiegende AML-/GwG-Mängel, einen Cybervorfall-Meldungsverzug nach BAIT und potenzielle MAR-Verletzungen im Zusammenhang mit dem Eigenhandel in Token TN

aufgedeckt. Parallel laufen ein FIU-Verfahren und ein Strafverfahren gegen den CCO.

Die Kanzlei wurde am 20. März 2026 mandatiert und hat seitdem das Institut im gesamten Prüfungsverfahren begleitet. Die Stellungnahme zur Anhörung wurde am 28. Juli 2026 eingereicht.

II. Offene rechtliche Fragen und Risiken

A. Bußgeldverfahren (höchstes unmittelbares Risiko)

Das Bußgeldverfahren ist der unmittelbarste Risikofaktor. Die Einschätzung der Kanzlei:

- **Wahrscheinlichkeit Bußgeld:** Sehr hoch (über 90 %)
- **Erwartete Höhe bei Settlement:** EUR 1,5 Mio.
- **Erwartete Höhe ohne Settlement:** EUR 3,0-4,5 Mio.
- **Veröffentlichungsrisiko § 60b GwG:** Mittel (bei Settlement: reduziert)

B. MiCAR-CASP-Zulassung (strategisch wichtigstes Risiko)

Die MiCAR-Zulassung ist für das Geschäftsmodell des Instituts existenziell. Ohne CASP-Zulassung kann es nach dem 30. Juni 2026 keine Kryptoverwahrung mehr anbieten. Das Institut operiert derzeit im Grenzbereich des Übergangsregimes.

- **Wahrscheinlichkeit Zulassung bei gutem Settlement:** Mittel-hoch
- **Wahrscheinlichkeit Zulassung bei gescheitertem Settlement:** Niedrig-mittel
- **Fallback-Option:** Notfallplanung für geordnete Übertragung von Kundenvermögen an ein anderes CASP

C. MAR-Voruntersuchung Token TN (mittelfristiges Risiko)

Die BaFin-Voruntersuchung kann jederzeit in eine formelle Untersuchung überführt werden. Das Institut hat den Eigenhandel in Token TN eingestellt. Die Kanzlei wird ein externes Marktexpertengutachten beauftragen.

- **Wahrscheinlichkeit formeller Untersuchung:** Mittel (40 %)
- **Wahrscheinlichkeit Sanktionen bei Untersuchung:** Niedrig-mittel

D. Strafverfahren CCO (personelles und institutionelles Risiko)

Das Strafverfahren gegen Dr. Tannenfels ist vom Institut formal getrennt. Es besteht aber ein institutionelles Reputationsrisiko und die BaFin-Aufsicht könnte die CCO-Besetzung neu bewerten.

- **Empfehlung der Kanzlei:** Aufsichtsrat sollte über Abberufung und Neubesetzung des CCO-Postens entscheiden, unabhängig vom Ausgang des Strafverfahrens.

III. Empfehlungen der Kanzlei

1. **Settlement beschleunigen:** Bilateral-Gespräch mit BaFin muss bis Ende August 2026 geführt werden; Settlement-Angebot bis 15. September 2026 einreichen.
2. **KPMG-Mandat bestätigen:** Die externe AML-Prüfung durch KPMG ist entscheidend für die Glaubwürdigkeit der Remediation gegenüber der BaFin.
3. **CCO-Nachfolge regeln:** Neubesetzung des CCO-Postens mit einem ausgewiesenen GwG/MiCAR-Experten ohne strafrechtliche Vorbelastung.

4. **MiCAR-Projektteam verstärken:** Die drei ausstehenden Token-White-Papers und die TFR-Compliance müssen bis 31. Oktober 2026 abgeschlossen sein.

5. **Pressestrategie finalisieren:** Pressemitteilung muss synchron mit BaFin-Entscheid vorbereitet sein; proaktive Kommunikation gegenüber Kernkunden (Top 10 nach AuM) durch CEO empfohlen.

IV. Gebührenprognose

Geleistete Stunden bis 10. August 2026: rd. 380 Stunden (rd. EUR 187.000 zzgl. MwSt.) Erwartete weitere Stunden bis Mandatsabschluss (inkl. Settlement-Verhandlung): rd. 150 Stunden (rd. EUR 75.000 zzgl. MwSt.) Gesamthonorar geschätzt: EUR 262.000 bis EUR 310.000 zzgl. MwSt.

Frankfurt am Main, 10. August 2026

Prof. Dr. Heinrich Schwertbeck Rechtsanwalt, Bankaufsichtsrecht Schwertbeck Roosendaal mbB Mainzer Landstraße 172 60327 Frankfurt am Main

E-Mails

Datei: emails/email-bafin-pruefungsmitteilung.eml

Von	bafin-vbs4@bafin.de
An	vorstand@thalvenia-bank.de
Datum	Wed, 18 Mar 2026 09:22:11 +0100
Betreff	Sonderpruefung gem. 44 KWG - Az. VBS 4 1 7-K-22-188/2026 - Pruefungsmitteilung

Bundesanstalt fuer Finanzdienstleistungsaufsicht (BaFin)
Referat VBS 4 - Kreditinstitutsaufsicht Spezialinstitute
Graurheindorfer Str. 108
53117 Bonn

An den
Vorstand der Thalvenia Bank AG
Koenigstrasse 87
70173 Stuttgart

Stuttgart/Bonn, 18. Maerz 2026

Aktenzeichen: VBS 4 1 7-K-22-188/2026
Bearbeiterin: Dr. Hannelore Koesters

Betreff: Anordnung einer Sonderpruefung nach § 44 Abs. 1 KWG

Sehr geehrter Herr Dr. Thalheim-Lattermann,
sehr geehrte Vorstandsmitglieder,

die Bundesanstalt fuer Finanzdienstleistungsaufsicht (BaFin) ordnet hiermit eine
Sonderpruefung der Thalvenia Bank AG gemaess § 44 Abs. 1 KWG i.V.m. § 44c KWG an.

PRUEFUNGSGEGENSTAND:

1. Interne Sicherungsmassnahmen zur Verhinderung von Geldwaesche und Terrorismusfinanzierung (§§ 4-12, 43 GwG)
2. Umsetzung der Bankaufsichtlichen Anforderungen an die IT (BAIT 2024), insbesondere Tz. 55 (Anzeigespflicht IT-Sicherheitsvorfaelle)
3. Marktintegritaet / MAR-Compliance (VO (EU) 596/2014 analog Art. 89 MiCAR)
4. Organisationspflichten nach MaRisk BA 2024 (AT 4.3, AT 7.1)

PRUEFER:

- Dr. Hannelore Koesters (Pruefungsleitung, VBS 4)
- Markus Pelzer (IT-Sicherheit, Referat IT-Aufsicht)
- Annika Wunderwald (AML/GwG, Referat GW 2)
- Rolf Sandkamp (Marktintegritaet, Referat WA 23)

PRUEFUNGSBEGINN: 20. April 2026 (Vor-Ort-Pruefung)

VORANFORDERUNG DOKUMENTE:

Innerhalb von 10 Werktagen ab Zugang dieses Schreibens sind der BaFin zu uebermitteln:

- GwG-Sicherungsmassnahmen-Dokumentation (vollstaendig)
- KYC-Akten aller Hochrisikokunden (Kategorie 3 und 4)
- PEP-Screening-Dokumentation der letzten 24 Monate

- STR-Meldeverzeichnis § 43 GwG
- IT-Sicherheitsberichte und Vorfallsmeldebuch
- Handelsarchiv Token TN (Oktober 2024 bis Januar 2026)

Das Institut hat die Pruefung zu unterstuetzen und allen Pruefern uneingeschraenkten Zugang zu Raeumlichkeiten, Systemen und Mitarbeitern zu gewaehren (§ 44 Abs. 1 S. 3 KWG).

Mit freundlichen Gruessen

Dr. Hannelore Koesters
Bundesanstalt fuer Finanzdienstleistungsaufsicht
Referat VBS 4

--

BaFin | Graurheindorfer Str. 108 | 53117 Bonn | www.bafin.de

Datei: emails/email-bnetza-cybersicherheits-zustaendigkeit.eml

Von	kritis@bundesnetzagentur.de
An	m.hoffrath-seel@thalvenia-bank.de
Datum	Fri, 03 Apr 2026 10:15:44 +0200
Betreff	Anfrage: Einstufung als KRITIS-Betreiber gem. BSI-KritisV - Az. BNetzA 7-K-2026-1847

Bundesnetzagentur
Referat 704 - Informationssicherheit kritischer Infrastrukturen
Tulpenfeld 4
53113 Bonn

An die
Leiterin Rechtsabteilung
Thalvenia Bank AG
Koenigstrasse 87
70173 Stuttgart

Bonn, 3. April 2026

Aktenzeichen: BNetzA 7-K-2026-1847

Bearbeiter: Dipl.-Ing. Rainer Luecke

Betreff: Anfrage zur moeglichen KRITIS-Einstufung und NIS2-Meldepflichten

Sehr geehrte Frau Dr. Hoffrath-Seel,

der Bundesnetzagentur ist bekannt, dass die Thalvenia Bank AG im Januar 2026 von einem IT-Sicherheitsvorfall (Ransomware) betroffen war. Eine entsprechende Meldung ist bei uns nicht eingegangen.

Wir bitten Sie, uns folgende Fragen zu beantworten:

1. KRITIS-Einstufung:

Unterschreitet die Thalvenia Bank AG den in der BSI-KritisV Anlage 1 Sektor Finanzen genannten Schwellenwert (Bilanzsumme EUR 30 Mrd.)? Falls ja, besteht keine Meldepflicht nach § 8b BSIG.

2. NIS2-Meldepflicht:

Das NIS2-Umsetzungsgesetz (in Kraft seit Oktober 2024) erfasst "wichtige Einrichtungen"

im Finanzsektor ohne Schwellenwert-Ausnahme. Bitte teilen Sie uns mit, ob Ihr Institut eine Erstmeldung nach § 32 BSIG erstattet hat oder eine Meldung beabsichtigt.

3. Koordination mit BaFin:

Soweit eine parallele BAIT-Meldung an die BaFin erfolgt ist, genuegt ein einfacher Verweis. Die Bundesnetzagentur koordiniert mit der BaFin gemaess MoU vom Juni 2024.

Bitte antworten Sie innerhalb von zwei Wochen ab Zugang dieses Schreibens.

Mit freundlichen Gruessen

Dipl.-Ing. Rainer Luecke
Bundesnetzagentur - Referat 704
Tel.: +49 228 14 80-0

--

Bundesnetzagentur | Tulpenfeld 4 | 53113 Bonn | www.bundesnetzagentur.de

Datei: emails/email-cybersicherheits-vorfall-meldung-bait.eml

Von	m.thorvaldsson@thalvenia-bank.de
An	m.vellbruck@thalvenia-bank.de
Datum	Fri, 09 Jan 2026 08:35:17 +0100
Betreff	NOTFALL - IT-Sicherheitsvorfall Stufe 2 - Ransomware 09.01.2026

IT-NOTFALL STUFE 2 - INTERNE MELDUNG (VERTRAULICH)

Zeitpunkt: 09. Januar 2026, 08:35 Uhr

Von: Magnus Thorvaldsson (CISO)

An: Vorstand, CRO, CCO, Leiterin Rechtsabteilung

LAGEBESCHREIBUNG:

Heute Nacht wurde unser Verwaltungsnetz durch einen Ransomware-Angriff befallen.
14 Server wurden verschluesselt. Der Angreifer nutzte CVE-2024-21762 (FortiGate VPN).

AKTUELLE SITUATION:

- Produktionssysteme: NICHT betroffen (Cold Custody physisch isoliert)
- MPC-Signing-Service: AUSGEFALLEN (Wiederherstellung in 12-18 Stunden erwartet)
- Kundenfonds: GESICHERT (Hot Wallets und Cold Storage unbeeintraehtigt)
- Loesegeldforderung: 35 Bitcoin (Zahlung NICHT empfohlen)
- Forensik-Team extern: CyberTrust GmbH Frankfurt - Einsatz beauftragt fuer 10:00 Uhr

BEREITS ERGRIFFENE MASSNAHMEN:

- Isolierung betroffener Netzwerksegmente (07:45 Uhr)
- FortiGate Notfallpatch eingespielt (08:20 Uhr)
- Backup-Verifikation laeuft

ZU KLAERENDE FRAGE:

Meldepflicht nach BAIT Tz. 55 (BaFin) und ggf. NIS2 (BSI):

Wann und was melden wir? Ich empfehle, den Anwalt hinzuzuziehen und erst nach Vorliegen der ersten Forensikergebnisse zu melden (Zeitraum: ca. 48-72h).

NAECHSTE SCHRITTE:

- Vorstandsmeeting 10:00 Uhr (Konferenzraum 2)
- Forensik-Beginn 11:00 Uhr

- Erste Lageeinschaetzung Forensik: ca. 13.01.2026

Magnus Thorvaldsson
Chief Information Security Officer (CISO)
Thalvenia Bank AG

Datei: emails/email-fiu-anfrage-stra.eml

Von	fiu-anfragen@zoll.bund.de
An	vorstand@thalvenia-bank.de
Datum	Sun, 22 Feb 2026 14:05:33 +0100
Betreff	Auskunftsersuchen gem. § 30 GwG - Az. 2026-FIU-7711-TN

Financial Intelligence Unit (FIU) Deutschland
Bundeszollamt - Zentralstelle fuer Finanztransaktionsuntersuchungen
Carusufer 3-5
01099 Dresden

An den
Vorstand der Thalvenia Bank AG
Koenigstrasse 87
70173 Stuttgart

Dresden, 22. Februar 2026

Aktenzeichen: 2026-FIU-7711-TN
Sachbearbeiterin: Kriminalhauptkommissarin Dorothea Pfeil

Betreff: Auskunftsersuchen gemaess § 30 GwG

Sehr geehrte Damen und Herren,

die Financial Intelligence Unit (FIU) richtet ein Auskunftsersuchen nach § 30 GwG an Ihr Institut. Dieser Vorgang ist streng vertraulich. Eine Information von Kunden oder Dritten ist nach § 44 GwG (Verbot der Informationsweitergabe) unzuessaessig und kann strafbar sein.

AUSKUNFTSGEGENSTAND:

Die FIU ersucht um Auskunft zu Transaktionen im Zeitraum Oktober 2024 bis Januar 2026, die den Kryptowert Token TN betreffen, insbesondere:

1. Vollstaendige Transaktionsdaten (Datum, Volumen, Gegenseite, Wallet-Adressen) fuer alle Kundentransaktionen in Token TN
2. KYC-Dokumentation fuer die Kunden mit internen Kennungen HR-07 und HR-11
3. Interne Verdachtsanalysevermerke fuer Token-TN-Transaktionen im Pruefrum
4. Risikoklassifizierung der Kunden HR-07 und HR-11 gemaess internem Ratingsystem

FRIST: Die Auskunft ist innerhalb von 15 Werktagen ab Zugang dieses Schreibens zu erteilen.

Die FIU weist darauf hin, dass eine Verletzung des Auskunftsersuchens nach § 30 Abs. 5 GwG als Ordnungswidrigkeit mit Bussgeld belegt werden kann.

Mit freundlichen Gruessen

KHK Dorothea Pfeil
Financial Intelligence Unit (FIU) Deutschland

Zentralstelle fuer Finanztransaktionsuntersuchungen

--

FIU | Carusufer 3-5 | 01099 Dresden | fiu@zoll.bund.de

Datei: emails/email-vorstand-thalvenia-an-kanzlei.eml

Von	c.thalheim-lattermann@thalvenia-bank.de
An	schwertbeck@schwertbeck-roosendaal.de
Datum	Wed, 18 Mar 2026 17:44:28 +0100
Betreff	DRINGEND - BaFin Sonderpruefung - Mandatsanfrage

Sehr geehrter Herr Professor Schwertbeck,

ich wende mich in einer aeusserst dringenden Angelegenheit an Sie.

Wir haben heute Morgen, 18. Maerz 2026, eine Sonderpruefungsmitteilung der BaFin erhalten (Az. VBS 4 1 7-K-22-188/2026). Die Pruefung betrifft unser gesamtes AML-System, unsere IT-Sicherheit nach BAIT und - ich schreibe das nur fuer Sie - auch Handelsaktivitaeten in einem bestimmten Kryptowert.

Ich habe Ihren Namen von der GDV-Tagung in Frankfurt. Sie sind der fuehrende Spezialist fuer Bankaufsichtsrecht bei Kryptoinstituten.

Folgender Hintergrund, streng vertraulich:

1. Im Januar hatten wir einen Cybervorfall (Ransomware), den wir etwas spaeter als vorgesehen an die BaFin gemeldet haben. Das wird ein Thema sein.
2. Unser CCO Herr Dr. Tannenfels wird von der Staatsanwaltschaft Stuttgart im Zusammenhang mit Geldwaeschevoruerfen ermittelt (§ 261 StGB). Das ist getrennt vom BaFin-Verfahren, haengt aber zusammen.
3. Die MiCAR-Lizenz, fuer die wir seit November 2024 beim Referat WA 37 beantragt haben, steht auf dem Spiel.

Wir verwalten EUR 4,3 Mrd. Kundenkryptoassets. Das ist kein Routinefall.

Koennen Sie morgen, 19. Maerz, nach Stuttgart kommen? Wir sind ab 9 Uhr verfuegbar und wuerden gerne alle vier Vorstandsmitglieder in einem Erstgespraech zusammenfassen. Bitte sagen Sie mir sofort telefonisch oder per Mail Bescheid.

Mit freundlichen Gruessen

Dr. Cornelius Thalheim-Lattermann
CEO / Vorstandsvorsitzender
Thalvenia Bank AG
Koenigstrasse 87
70173 Stuttgart
Tel.: +49 711 4922-100

Excel-Tabellen

Datei: xlsx/gwg-pflichten-katalog.xlsx

Tabellenblatt: GwG-Pflichten

GwG-Pflichtenkatalog Thalvenia Bank AG - BaFin-Sonderprüfung 18 8-K-22-2026									
	Pflicht	GwG-Paragraf	Status Thalvenia	Befund BaFin	Frist	Massnahme	Verantwortlich	Status	Anmerkung
	Risikoanalyse	§ 5 GwG	Vorhanden, veraltet (2023)	Wesentlich: keine Aktualisierung 2024/2025	30.06.2026	Aktualisierung Risikoanalyse	CCO	Abgeschlossen	Genehmigt durch Vorstand 30.06.2026
	Organisationische Pflichten	§ 6 GwG	CCO bestellt, Schulungsplan vorhanden	Schulungsplan nicht vollständig umgesetzt	31.08.2026	Schulungsquote auf 100% erhöhen	CCO/HR	Abgeschlossen	Schulungsquote 100% seit Juni 2026
	Beauftragtenbenennung	§ 7 GwG	CCO Dr. Tannenfels benannt	Vertretungsregelung unzureichend	15.08.2026	Formelle Stellvertreter-Benennung	Vorstand/CCO	In Bearbeitung	Strafverfahren gegen CCO beachten
	Allg. Sorgfaltspflichten	§ 10 GwG	KYC-Prozess existiert	8 Hochrisikokunden: 5 schwerwiegende Mängel	30.09.2026	KYC-Nacherfüllung aller HR-Kunden	CCO/AML-Team	Teilweise	HR-03/07/09 abgeschlossen; HR-11/19 offen
	Wirtschaftl. Berechtigte	§ 3/§ 10 GwG	Grundsätzlich vorhanden	HR-03: WiB nicht festgestellt	30.06.2026	WiB-Feststellung HR-03	AML-Team	Abgeschlossen	WiB-Akte vollständig seit Juni 2026
	Vereinfachte Sorgfaltspf.	§ 14 GwG	Kategorisierung vorhanden	Kein Befund	-	Keine Massnahme erforderlich	-	OK	-

GwG-Pflichtenkata- log Thalvenia Bank AG - BaFin-Sonder- prüfung 18 8-K-22-2 026									
	Verstärkte Sorgfal- tspf.	§ 15 GwG	Nur teilweise angewan- dt	HR-07: M ittelherku- nft unklar; HR-09: L aenderris- iko ignoriert	30.09.20 26	Vollstän- dige Mitte- lherkunfts- -Doku	CCO/AM L-Team	In Bearbe- itung	HR-07 N acherfuell- ung läuft
	PEP-Screening	§ 15 Abs. 3 GwG	SymphonyAI Tier 1 (unzureichend)	3 PEPs nicht erkannt (HR-11, HR-23, HR-31)	30.04.20 26	Upgrade auf Tier 2; retrogr- ade Prüfung	CCO/IT	Abgeschl- ossen	Tier-2-Ver- trag seit April 2026
	PEP-GF- Genehmi- gung	§ 15 Abs. 5 Nr. 2 GwG	Fehlte bei 3 Kunden	Formverl- etzung	31.05.20 26	GF-Gene- hmigung nachgeh- olt	CEO/CC O	Abgeschl- ossen	Genehmi- gungen n- achgeholt Mai 2026
	Mittelherk- unft PEP	§ 15 Abs. 5 Nr. 3 GwG	Fehlte bei HR-07	Schwerwi- gend	30.09.20 26	Vollstän- dige Mitte- lherkunfts- -Doku HR-07	CCO/AM L	In Bearbe- itung	Schwierig wegen Li- echtenste- in-Stiftun- g
	Verstärkte Ueber- wachung PEP	§ 15 Abs. 5 Nr. 4 GwG	Nicht aktiviert bei 3 Kunden	Mittelsch- wer	30.05.20 26	Verstärkte Ueber- wachung aktiviert	AML-Tea- m	Abgeschl- ossen	Monitorin- g aktiv seit Mai 2026
	Transakti- onsmonit- oring	§ 25h KWG analog	Chainaly- sis Reactor v- orhanden	Regelwer- k seit 2022 nicht aktu- alisiert	31.08.20 26	Regelwer- k-Aktualis- ierung	CCO/IT	In Bearbe- itung	Fertigstell- ung August 2026
	Verdachts- meldepflicht	§ 43 GwG	3 STRs erstattet	5 weitere mögliche STR-Pflicht- verletzungen	Sofort bei Verdacht	Nachprü- fung 5 Tr- ansaktionen	CCO/Leg- al	In Prüfung	Kanzlei bewertet Pflichtver- letzung
	STR-Dok- umentati- on	§ 43 Abs. 2 GwG	Vermerke vorhanden	Qualität der Vermerke unzureichend	30.09.20 26	STR-Dok- umentati- onsstand erhöhen	CCO	Geplant	Teil AML- Handbuc- h v3.4

GwG-Pflichtenkatalog Thalvenia Bank AG - BaFin-Sonderprüfung 188-K-22-2026									
	Tipping-off-Verbot	§ 44 GwG	Policy vorhanden	Kein Befund	-	Keine Massnahme erforderlich	-	OK	Policy korrekt angewandt bei FIU-Verfahren
	Aufbewahrungspflichten	§ 8 GwG	5-Jahres-Archiv	Kein Befund	-	Keine Massnahme erforderlich	-	OK	Elektronisches Archiv DSGVO-konform
	AML-Schulung	§ 6 Abs. 2 GwG	Jährliche Schulung	Schulungsquote 2025: nur 68%	30.06.2026	Pflichtteilnahme aller Mitarbeiter	CCO/HR	Abgeschlossen	100% Abdeckung seit Juni 2026
	Interne Revision AML	§ 6 Abs. 1 GwG	Revisionsberichte vorhanden	Letzter Revisionsbericht August 2024	31.10.2026	Interne Revision AML neu beauftragen	CRO/Revision	Geplant	Gekoppelt an KPMG-Auftrag
	KPMG externe Prüfung	Settlement-Undertaking	Beauftragung abgeschlossen	BaFin-Settlement-Vereinbarung	31.10.2026	KPMG-Bericht vorlegen	CRO	In Beauftragung	Beauftragung KPMG August 2026
	MiCAR AML-Pflichten	Art. 92 MiCAR	Teilweise umgesetzt	TFR Travel Rule nicht vollständig	31.10.2026	TFR-Compliance implementieren	CCO/IT	Geplant	Frist MiCAR-Umsetzung
	Risikoanalyse MiCAR	Art. 92 MiCAR i.V.m. § 5 GwG	Aktualisiert Juni 2026	MiCAR-spezifische Risiken jetzt enthalten	-	Jährliche Aktualisierung einplanen	CCO	Abgeschlossen	Eingeschlossen in neue Risikoanalyse
	Interessenkonflikte	Art. 72 MiCAR	Policy vorhanden, Krypto-Eigenhandel fehlte	Eigenhandel Token TN nicht erfasst	31.08.2026	Policy-Ergänzung um Krypto-Eigenhandel	CCO/Legal	In Bearbeitung	Token-TN-Eigenhandel eingestellt
	NPP Neue Produkte	MaRisk AT 8.1	NPP-Prozess vorhanden	Token TN ohne NPP gestartet	30.04.2026	NPP-Nachholung Token TN	CRO/CCO	Abgeschlossen	CRO-Freigabe und Risikokomitee-Beschluss April 2026

GwG-Pflichtenkata- log Thalvenia Bank AG - BaFin-Sonder- prüfung 18 8-K-22-2 026									
	Handelsli- mits	MaRisk BTO 3	Fuer Token TN nicht vorhande- n	Handelsli- mit fehlte	30.04.20 26	Positionsl imit EUR 10 Mio. ei- ngefuehrt	CRO	Abgeschl- ossen	Stop-Los- s -15% aktiviert
	Zweivote- n-System Handel	MaRisk AT 4.3.3	Fehlte fuer Krypt- owerte	Kein Zwe- ivoten bei Token TN	31.07.20 26	Zweivote- n-System implemen- tiert	CRO/CF O	Abgeschl- ossen	Impleme- ntiert Juli 2026
	IT-Pruefb- ericht	Auflage BaFin 2020	2020-202 3 vorhan- den; 2024 fehlt	Wesentlic- h: Auflage nicht erfuellt	15.09.20 26	IT-Pruefb- ericht 2024 bea- uftragen	CTO	In Beauftr- agung	Beauftrag- ung abge- schlosse- n
	BAIT Notf- allkonzept	BAIT Tz. 49-54	Stand Oktober 2022, nicht MiC AR-konfo- rm	Veraltet	31.07.20 26	Ueberarb- eitung No- tfallkonze- pt	CTO/CIS O	Abgeschl- ossen	Neue Version Juli 2026
	BAIT Anz- eigepflich- t	BAIT Tz. 55	Meldung verspaedet (4 Tage statt 24h)	Schwerwi- egend: BAIT Tz. 55 verletzt	Sofort (a- bgeschlo- ssen)	SOC-Pro- zess ueb- erarbeitet	CISO	Abgeschl- ossen	Neue An- weisung seit Februar 2026
	BCM-Tes- ts	BAIT Tz. 49-54	Letzter Test August 2024 (18 Monate)	MPC-Sig- ning DR-Test ueberfael- lig	30.09.20 26	BCM-Tes- t MPC-Si- gning	CTO	Geplant	Test Sept- ember 2026 geplant
	Schwach- stellenma- nagement	BAIT Tz. 27	Kein formaler Prozess	CVE-202 4-21762 nicht gepatcht	31.07.20 26	Patch-SL A 72h for- malisiert	CISO	Abgeschl- ossen	SLA-Dok- ument ve- rabschied- et Juli 2026

Datei: xlsx/kundenidentifikation-kyc-mangelpruefung.xlsx

Tabellenblatt: KYC-Mangelpruefung

KYC-Mangelprüfung Hochrisikokunden - Thalvenia Bank AG - Stand August 2026								
	Kunde (anonym)	Risikoklasse	KYC-Beleg	Mangel	PEP-Status	Folgeschritt	Status	Anmerkung
	HR-01	4	Grundidentifizierung vorhanden; Organigramm 2023	Organigramm veraltet; § 10 Abs. 3 GwG	Nein	Aktuelles Organigramm anfordern	In Bearbeitung	Frist 31.08.2026
	HR-03	4	Grundidentifizierung; WiB-Akte unvollständig	WiB nicht festgestellt § 3/§ 10 GwG (schwer)	Nein	WiB-Feststellung abschliessen	Abgeschlossen	WiB vollständig seit Juni 2026
	HR-05	3	Vollständige KYC-Akte	Kein wesentlicher Befund	Nein	Keine Massnahme erforderlich	OK	Musterkunde fuer Compliance-Referenz
	HR-07	4	Grundidentifizierung; Mittelherkunft: einseitige Erklärung	Mittelherkunft unzureichend § 15 Abs. 4 GwG (schwer)	Nein, geprüft	Vollständige Mittelherkunfts-Dokumentation	In Bearbeitung	Liechtenstein-Stiftung; Anwalt eingeschaltet
	HR-09	4	Grundidentifizierung; nur Standardprüfung	Laenderisiko El Salvador ignoriert § 15 Abs. 3 GwG (schwer)	Nein	Verstärkte Sorgfaltspflichten nachholen	Abgeschlossen	Nacherfüllung abgeschlossen Juni 2026
	HR-11	3 -> 4	Grundidentifizierung 2022; PEP-Prüfung: kein Treffer	PEP nicht erkannt (georgischer Ministerialbeamter) § 15 Abs. 3 GwG (schwer)	JA (PEP Tier 2)	GF-Genehmigung nachgeholt; verstärkte Überwachung	Abgeschlossen	Tier-2-Screening hat PEP-Status bestätigt; Klasse hochgesetzt
	HR-15	3	Vollständige Akte; GF-Genehmigung fehlt	GF-Genehmigung fehlt § 15 Abs. 5 Nr. 2 GwG (mittel)	Nein	GF-Genehmigung nachgeholt	Abgeschlossen	Cayman Islands: Hochrisikodritland

KYC-Mangelprüfung Hochrisikokunden - Thalvenia Bank AG - Stand August 2026								
	HR-19	3	KYC-Akte Stand 2021 (5 Jahre veraltet)	Aktualisierungsintervall ueberschritten § 10 Abs. 3 GwG (schwer)	Nein	Vollstaendige KYC-Aktualisierung	In Bearbeitung	Singapur; EUR 8,4 Mio. Transaktionen 2025
	HR-23	3 -> 4	Grundidentifizierung 2023; PEP-Pruefung: kein Treffer	Moldauischer Buergemeister a.D. nicht erkannt § 15 Abs. 3 GwG (schwer)	JA (PEP kommunal)	GF-Genehmigung; verstärkte Ueberwachung	Abgeschlossen	Retrograde PEP-Pruefung Mai 2026
	HR-31	3 -> 4	Grundidentifizierung 2024; PEP-Pruefung: kein Treffer	Nordmazed. Richter Oberstes Gericht nicht erkannt § 15 Abs. 3 GwG (schwer)	JA (PEP Justiz)	GF-Genehmigung; verstärkte Ueberwachung	Abgeschlossen	Retrograde PEP-Pruefung Mai 2026
	HR-37	3	Vollstaendige Akte; aktuell	Kein wesentlicher Befund	Nein	Keine Massnahme erforderlich	OK	Standardprozess korrekt angewandt
	HR-42	4	WiB identifiziert; Aktualisierung 2024	Teilweise veraltet (12 Monate)	Nein	Aktualisierung beauftragen	In Bearbeitung	Laeuft regulaer
	HR-45	4	Grundidentifizierung vorhanden	Herkunft Kryptofonds unklar	Nein, in Pruefung	Herkunftsnaachweis anfordern	In Bearbeitung	Kryptofonds Herkunft: On-Chain-Analyse
	HR-51	3	Vollstaendige Akte	Kein Befund	Nein	Keine Massnahme	OK	Routinefall
	HR-58	4	Identifizierung 2021; keine Aktualisierung	4 Jahre ohne Aktualisierung; Hochrisiko § 10 Abs. 3 GwG	Nein	Vollstaendige KYC-Aktualisierung	In Bearbeitung	Priorisiert nach HR-19

Word-Dokumente

Datei: docx/compliance-handbuch-thalvenia-v3-3.docx

Compliance-Handbuch Thalvenia Bank AG

Version 3.3 - Stand: Oktober 2025

Vertraulich - Nur fuer interne Verwendung

1. Geltungsbereich und Grundsätze

Dieses Handbuch gilt fuer alle Mitarbeiterinnen und Mitarbeiter der Thalvenia Bank AG. Es legt die Grundsätze der Compliance-Organisation, die Pflichten aus dem Geldwaeschegesetz (GwG), den bankaufsichtlichen Anforderungen (MaRisk BA 2024, BAIT 2024) sowie aus der MiCAR-Verordnung (VO (EU) 2023/1114) fest.

2. AML-Organisation

2.1 Geldwaeschebeauftragter

Geldwaeschebeauftragter i.S.d. § 7 GwG ist der Chief Compliance Officer (CCO). Er ist unmittelbar dem Vorstand unterstellt und weisungsunabhaengig in seiner Meldefunktion. Stellvertreter ist die AML-Analystin Lena Goebel-Strauch.

2.2 Kundensorgfaltspflichten (§§ 10-15 GwG)

Jeder Neukunde ist zu identifizieren. Bei Hochrisikokunden (Kategorie 3 und 4) sind verstaerkte Sorgfaltspflichten nach § 15 GwG anzuwenden. Die PEP-Pruefung erfolgt mittels SymphonyAI Sensa (Tier 1 + Tier 2 seit April 2026).

2.3 Verdachtsmeldepflicht (§ 43 GwG)

Bei Verdacht auf Geldwaesche oder Terrorismusfinanzierung ist unverzueglich eine Meldung an die FIU zu erstatten. Die Meldung erfolgt ueber das goAML-Portal. Der Geldwaeschebeauftragte entscheidet ueber die Erstattung. Alle Analyse-Vermerke sind aktenkundig zu machen.

3. IT-Sicherheit (BAIT 2024)

3.1 Anzeigepflicht IT-Sicherheitsvorfaelle (BAIT Tz. 55)

Wesentliche IT-Sicherheitsvorfaelle sind der BaFin unverzueglich, spaetestens 24 Stunden nach Kenntniserlangung, zu melden. Eine 'wesentliche IT-Sicherheitsvorfall' liegt vor, wenn die Vertraulichkeit, Integritaet oder Verfuegbarkeit von Kundendaten, Kundenvermoegenswerten oder kritischen Systemen beeintraehtigt ist. Der CISO meldet unmittelbar an Vorstand und BaFin.

3.2 Business Continuity Management

Das Notfallkonzept (Stand: Juli 2026) legt DR-Prozesse fuer alle kritischen Systeme (MPC-Signing, Cold Custody, Core Banking) fest. DR-Tests erfolgen halbjaehrlich. Patches fuer kritische Schwachstellen (CVSS > 9.0) sind innerhalb von 72 Stunden einzuspielen.

4. MiCAR-Compliance

Als CASP-Antragsteller nach VO (EU) 2023/1114 beachtet das Institut bereits die MiCAR-Anforderungen an Governance (Art. 68), Interessenkonflikte (Art. 72), Eigenkapital (Art. 67) und Marktmissbrauch (Art. 89-92). White Papers fuer neue Kryptowertarten sind vor Aufnahme des Verwahrungsgeschaefts zu

erstellen und der BaFin vorzulegen.

5. Schulung und Kultur

Alle AML-relevanten Mitarbeiter erhalten jaehrlich eine Pflichtschulung zu GwG, Sanktionsrecht und BAIT-Anforderungen. Die Schulungsquote muss 100 % betragen; Nichterfuellung ist dem CCO und dem Vorstand zu melden.

Dieses Handbuch ersetzt Version 3.2 (Maerz 2024). Version 3.4 ist in Erarbeitung (geplant Oktober 2026).

Datei: docx/pressemitteilung-entwurf.docx

PRESSEMITTEILUNG — ENTWURF

NICHT ZUR VEROEFFENTLICHUNG — INTERNE ABSTIMMUNG

Thalvenia Bank AG Stuttgart

Stuttgart, [Datum einfuegen nach BaFin-Entscheid]

Thalvenia Bank AG kommuniziert Massnahmen zur Compliance-Staerkung

Die Thalvenia Bank AG (Thalvenia), eines der fuehrenden deutschen Spezialinstitute fuer institutionelle Kryptoverwahrung, gibt im Zusammenhang mit der im Maerz 2026 eingeleiteten Sonderpruefung durch die Bundesanstalt fuer Finanzdienstleistungsaufsicht (BaFin) folgende Erklaerung ab.

Ueber die BaFin-Pruefung

Im Rahmen der regulaeren Aufsichtsmaessnahmen wurde die Thalvenia Bank AG einer Sonderpruefung nach § 44 KWG unterzogen. Die Pruefung hat Verbesserungsbereiche identifiziert, die das Institut unverzueglich adressiert hat.

Massnahmen

Seit Maerz 2026 hat Thalvenia ein umfassendes Compliance-Staerkungsprogramm aufgelegt: Aktualisierung der Geldwaescherisikoanalyse, Ausbau des PEP-Screenings, Ueberarbeitung der IT-Sicherheitsprozesse und 100 prozentige AML-Schulungsabdeckung.

"Wir nehmen regulatorische Anforderungen sehr ernst und haben die identifizierten Verbesserungsbedarfe umgehend adressiert. Die Sicherheit der Kundenvermoegenswerte war zu keiner Zeit gefaehrdet", erklaert CEO Dr. Cornelius Thalheim-Lattermann.

MiCAR-Zulassung

Thalvenia beantragte im November 2024 die Zulassung als Crypto-Asset Service Provider (CASP) nach MiCAR. Das Verfahren laeuft regulaer.

Kundenvermoegenswerte

Die verwalteten Kundenvermoegenswerte in Hoehe von EUR 4,3 Mrd. waren zu keinem Zeitpunkt gefaehrdet.

Ueber Thalvenia Bank AG

Die Thalvenia Bank AG ist ein Stuttgarter Spezialinstitut fuer institutionelle Kryptoverwahrung mit BaFin-Zulassung seit Oktober 2020. Das Institut verwaltet Kryptovermoegenswerte fuer institutionelle Anleger in Deutschland, der Schweiz und Oesterreich.

Medienkontakt:

Pressestelle Thalvenia Bank AG

Tel.: +49 711 4922-200

presse@thalvenia-bank.de

HINWEIS: Entwurf vom 2. August 2026. Freigabe durch Vorstand, Aufsichtsrat und Kanzlei Schwertbeck Roosendaal erforderlich. Veroeffentlichungszeitpunkt: nach BaFin-Entscheid.

Datei: docx/stellungnahme-vorstand-thalvenia-bafin-pruefung.docx

Thalvenia Bank AG

Stellungnahme des Vorstands zur BaFin-Anhoerung

Az. BaFin VBS 4 1 7-K-22-188/2026

Datum: 28. Juli 2026

Absender: Thalvenia Bank AG, vertreten durch den Vorstand

Adressat: Bundesanstalt fuer Finanzdienstleistungsaufsicht, Referat VBS 4

Bearbeitung: Schwertbeck Roosendaal mbB, Frankfurt am Main (Az. SR-2026-FIN-0612)

I. Vorbemerkung

Die Thalvenia Bank AG begruesst die Moeglichkeit zur Stellungnahme nach § 28 Abs. 1 VwVfG. Der Vorstand nimmt die im Anhoerungsschreiben vom 14. Juli 2026 festgestellten Maengel ernst und hat umfangreiche Abhilfemassnahmen ergriffen.

II. Zum Cybervorfall Januar 2026

Das Institut erkennt an, dass die BaFin-Meldung vom 13. Januar 2026 die Frist des BAIT Tz. 55 nicht einhielt. Es handelte sich um eine Fehlklassifizierung beim initialen SIEM-Alarm um 02:17 Uhr, nicht um eine bewusste Fristversaenus.

Der SOC-Mitarbeiter im Schichtbetrieb bewertete den Alarm aufgrund einer Aehnlichkeit mit bekannten Fehlalarmustern als False Positive. Erst mit der Entdeckung verschluesselter Server um 08:10 Uhr war eine zuverlaessige Klassifizierung moeglich.

Das Institut hat seitdem alle SOC-Eskalationsprozesse ueberarbeitet. Die neue interne Anweisung verpflichtet zur sofortigen BaFin-Meldung ab Inkrafttreten des IT-Notfalls Stufe 2, unabhaengig vom Informationsstand.

III. Zu den AML/KYC-Maengeln

Die festgestellten KYC-Luecken werden grundsatzlich eingeraeumt. Fuer Kunde HR-03 (fehlende WiB-Feststellung) wurde die Nacherfuellung bereits vor der Sonderpruefung eingeleitet (August 2025).

Hinsichtlich des PEP-Screening-Mangels (Kunden HR-11, HR-23, HR-31) war das Institut auf die Tier-1-Abdeckung des SymphonyAI-Systems angewiesen, die dem branchenueblichen Standard entsprach. Das System wurde inzwischen auf Tier-2-Abdeckung aufgeruestet.

IV. Remediation-Massnahmen (Auswahl)

V. Bitte

Der Vorstand bittet die BaFin: (1) die Anordnung nach § 25a KWG auf noch ausstehende Massnahmen zu beschraenken; (2) beim Bussgeldverfahren die umfangreiche Remediation strafmildernd zu beruecksichtigen; (3) die MiCAR-Entscheidung nicht mit dem Bussgeldverfahren zu verknuepfen.

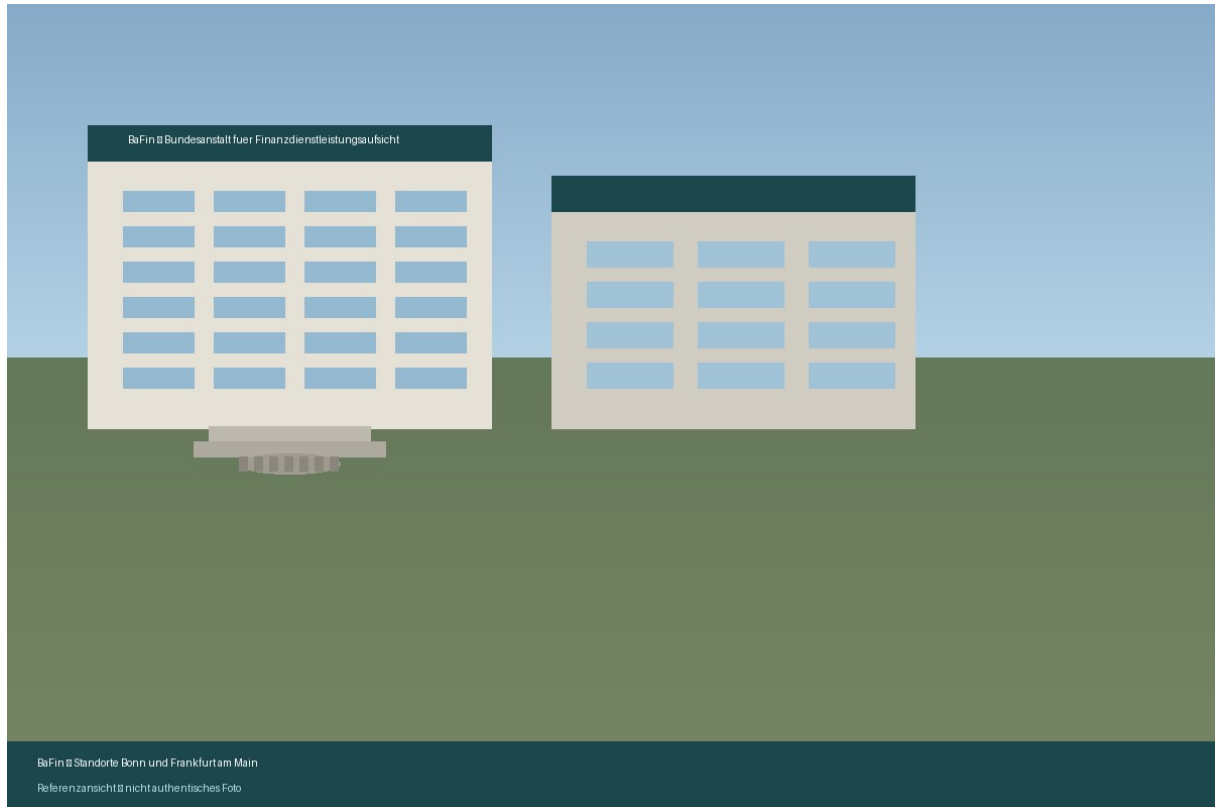
Frankfurt am Main / Stuttgart, 28. Juli 2026

Prof. Dr. Heinrich Schwertbeck
Schwertbeck Roosendaal mbB
(im Auftrag der Thalvenia Bank AG)

Massnahme	Status (28.07.2026)
Risikoanalyse § 5 GwG aktualisiert	Abgeschlossen 30.06.2026
KYC-Nacherfuellung HR-03, HR-07, HR-09	Abgeschlossen 30.06.2026
PEP-Datenbank-Upgrade Tier 2	Abgeschlossen April 2026
SOC-Eskalationsprozess ueberarbeitet	Abgeschlossen Februar 2026
BAIT-Notfallkonzept ueberarbeitet	Abgeschlossen Juli 2026
AML-Schulung 100 % Abdeckung	Abgeschlossen Juni 2026

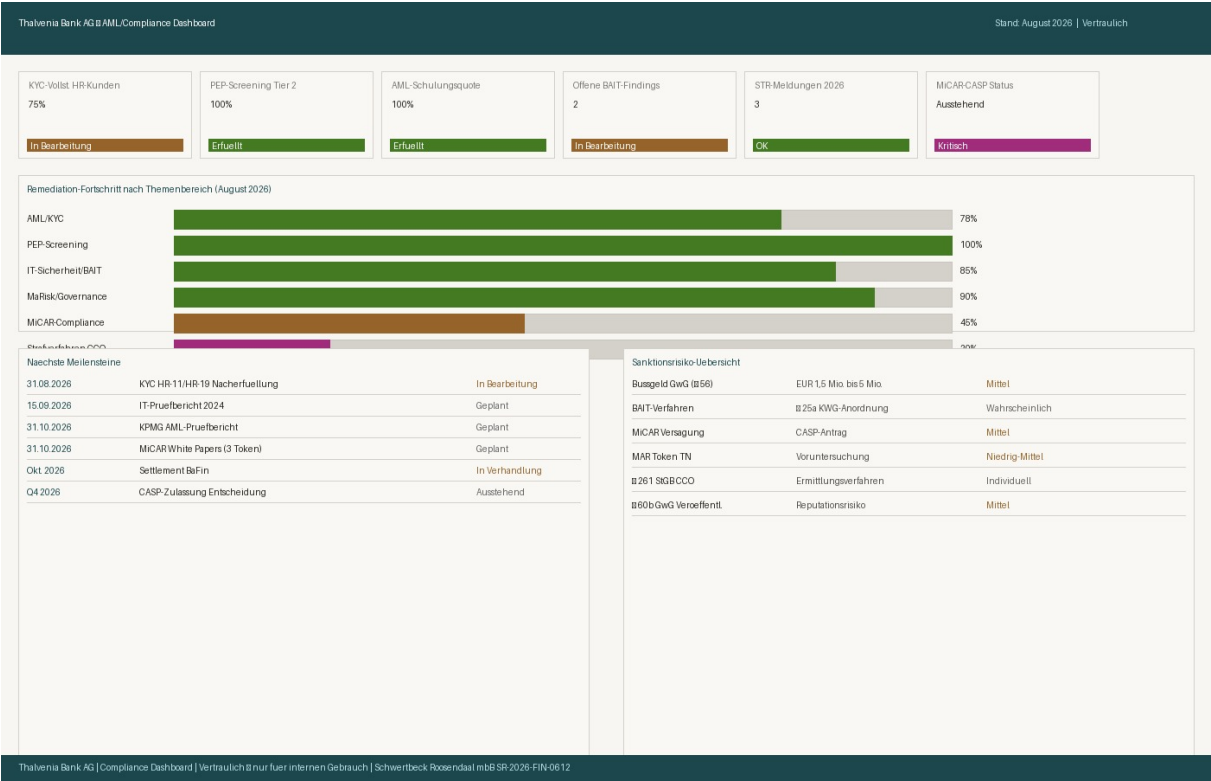
Bildanlagen und Screenshots

Datei: jpg/bafin-bonn-frankfurt-gebaeude.jpg



Bilddatei: bafin-bonn-frankfurt-gebaeude.jpg

Datei: jpg/compliance-dashboard-screenshot.jpg



Bilddatei: compliance-dashboard-screenshot.jpg

Datei: jpg/thalvenia-hauptsitz-stuttgart.jpg



Bilddatei: thalvenia-hauptsitz-stuttgart.jpg

PDF-Anhang: pdfs/compliance-handbuch-thalvenia-auszug.pdf

Datei: compliance-handbuch-thalvenia-auszug.pdf

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

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

Quellen:

[1] [GwG §§ 4-12, 43, 44: gesetzte-im-internet.de/gwg](#) | [2] [MaRisk BA 2024: bafin.de/MaRisk-2024](#) | [3] [BAIT 2024: bafin.de/BAIT](#) | [4] [MiCAR Art. 89-92: EUR-Lex MiCAR](#)

PDF-Anhang: pdfs/stellungnahme-bafin-final.pdf

Datei: stellungnahme-bafin-final.pdf

THALVENIA BANK AG

Stellungnahme zur BaFin-Anhoerung

Az. BaFin VBS 4 1 7-K-22-188/2026

Absender:	Thalvenia Bank AG, Koenigstrasse 87, 70173 Stuttgart
Adressat:	BaFin, Referat VBS 4, z.Hd. Dr. Hannelore Koesters
Vertreten durch:	Schwertbeck Roosendaal mbB, Frankfurt a.M. (Az. SR-2026-FIN-0612)
Datum:	28. Juli 2026
Bezug:	Anhoerungsschreiben BaFin vom 14. Juli 2026

I. Vorbemerkung

Die Thalvenia Bank AG begruesst die Moeglichkeit zur Stellungnahme nach § 28 Abs. 1 VwVfG. Der Vorstand nimmt die im Anhoerungsschreiben vom 14. Juli 2026 festgestellten Maengel ernst und hat seit Einleitung der Sonderpruefung umfangreiche Massnahmen ergriffen. Ziel dieser Stellungnahme ist es, zum einen tatsaechliche Unrichtigkeiten zu korrigieren und zum anderen den Stand der Remediation vollstaendig zu dokumentieren.

II. Zum Cybervorfall Januar 2026 (BAIT Tz. 55)

Das Institut erkennt an, dass die BaFin-Meldung vom 13. Januar 2026 die Frist des BAIT Tz. 55 nicht einhielt. Es handelte sich jedoch nicht um eine bewusste Fristversaemnis. Der SIEM-Alarm um 02:17 Uhr wurde vom SOC-Schichtmitarbeiter als False Positive klassifiziert. Erst nach Entdeckung der verschluesselten Server um 08:10 Uhr war eine zuverlaessige Klassifizierung als wesentlicher IT-Sicherheitsvorfall moeglich. Saemtliche SOC-Prozesse wurden seitdem ueberarbeitet. Eine neue interne Anweisung verpflichtet zur BaFin-Sofortmeldung ab IT-Notfall Stufe 2.

III. Zu den AML/KYC-Maengeln

Die festgestellten KYC-Luecken werden grundsatzlich eingeraeumt. Entlastungsgesichtspunkte: Fuer Kunde HR-03 wurde die Nacherfuellung bereits im August 2025 eingeleitet und lag zum Zeitpunkt der Pruefung vor. Fuer Kunde HR-07 entsprach die vorgelegte Mittelherkunftsdokumentation dem Marktstandard fuer liechtensteinische Stiftungen zum Onboarding-Datum 2020. Die PEP-Maengel sind auf unzureichende Datenbankabdeckung zurueckzufuehren; das Tier-2-Upgrade ist abgeschlossen.

IV. Remediation-Stand (Stand 28. Juli 2026)

Massnahme	Status
Risikoanalyse § 5 GwG aktualisiert und genehmigt	Abgeschlossen 30.06.2026

KYC-Nacherfuellung HR-03, HR-07, HR-09	Abgeschlossen 30.06.2026
PEP-Datenbank SymphonyAI Tier-2-Upgrade	Abgeschlossen April 2026
Retrograde PEP-Ueberpruefung alle HR-Kunden	Abgeschlossen Mai 2026
SOC-Eskalationsprozess ueberarbeitet	Abgeschlossen Februar 2026
BAIT-Notfallkonzept aktualisiert	Abgeschlossen Juli 2026
AML-Schulung 100% Abdeckung	Abgeschlossen Juni 2026
NPP Token TN nachgeholt; CRO-Freigabe	Abgeschlossen April 2026
Token-TN-Eigenhandel eingestellt	Abgeschlossen August 2026
KYC-Nacherfuellung HR-11, HR-19	In Bearbeitung (Frist 31.08.2026)
IT-Pruefbericht 2024	In Beauftragung (Frist 15.09.2026)

V. Bitte

Der Vorstand der Thalvenia Bank AG bittet die BaFin: (1) die Anordnung nach § 25a KWG auf die noch ausstehenden Massnahmen zu beschraenken; (2) beim Bussgeldverfahren die umfangreiche Remediation und den Erstverstoß strafmildernd zu beruecksichtigen; (3) die MiCAR-CASP-Entscheidung unabhaengig vom Bussgeldverfahren zu treffen.

Frankfurt am Main / Stuttgart, 28. Juli 2026

Prof. Dr. Heinrich Schwertbeck

Schwertbeck Roosendaal mbB

(im Auftrag der Thalvenia Bank AG)

Quellen und Rechtsgrundlagen:

[1] KWG § 25a, § 44: [gesetze-im-internet.de/kwg](https://www.gesetze-im-internet.de/kwg) | [2] GwG §§ 10, 15, 43: [gesetze-im-internet.de/gwg](https://www.gesetze-im-internet.de/gwg) | [3] MiCAR: [EUR-Lex 32023R1114](https://eur-lex.europa.eu/lexuris/ui/1114) | [4] BAIT: [bafin.de](https://www.bafin.de)