BaFin
Bundesanstalt für
Finanzdienstleistungsaufsicht

DEUTSCHE
BUNDESBANK
EUROSYSTEM

TLPT unter DORA

Testen der digitalen operationalen Resilienz

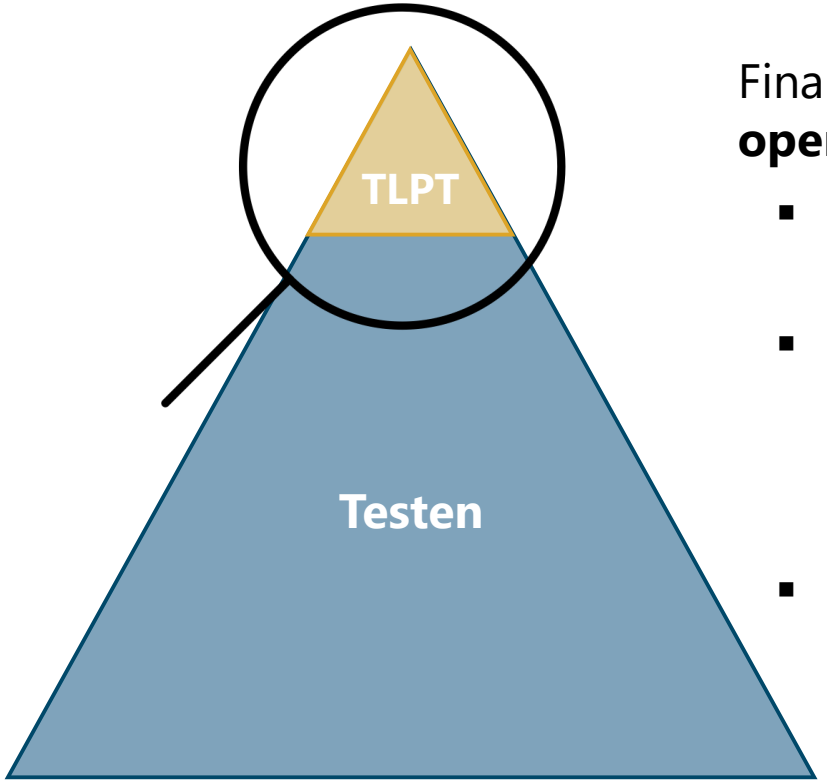
Testen der digitalen operationalen Resilienz

Etwas oder jemanden im Hinblick auf seine Beschaffenheit oder auf seine (vorgeschriebenen oder erwarteten) **Eigenschaften zu untersuchen**

Fähigkeit, die operative **Integrität** und **Betriebszuverlässigkeit** aufzubauen, zu gewährleisten und zu überprüfen, um die **Sicherheit** der Netzwerk- und Informationssysteme zu gewährleisten und die **kontinuierliche Erbringung** von Finanzdienstleistungen und deren **Qualität** zu unterstützen

Testen als ein Instrument für Finanzunternehmen (und die Aufsicht) zu überprüfen, ob das Ziel der digitalen operationalen Resilienz erreicht wird

Was fällt unter „Testen der digitalen operationalen Resilienz“ im Kontext von DORA?



DORA Kapitel IV (Artikel 24 bis 27) widmet sich exklusiv dem Testen

Finanzunternehmen haben ein **Programm für Tests der digitalen operationalen Resilienz** zu etablieren und zu pflegen. Das Testprogramm

- ist **integraler Bestandteil** des Risikomanagementrahmens für Informations- und Kommunikationstechnologien (IKT) (Art. 6(5) DORA)
- hat das **Ziel** IKT-Systeme, -Prozesse und Mitarbeitende auf die Effizienz der Fähigkeiten für Prävention, Erkennung, Reaktion und Wiederherstellung zu testen, um potentielle Schwachstellen aufzudecken und zu beseitigen
- umfasst eine **breite Palette** von Instrumenten und Maßnahmen:
  - von **grundlegenden Tests** von Schwachstellenbewertung und -scans, bis Penetrationstests für alle Finanzunternehmen (Art. 25 DORA)
  - bis zu **erweiterten Tests** wie TLPT - nur für Finanzunternehmen, die aus IKT-Perspektive ausgereift genug und von gewisser systemischer Relevanz sind (Art. 26 DORA)

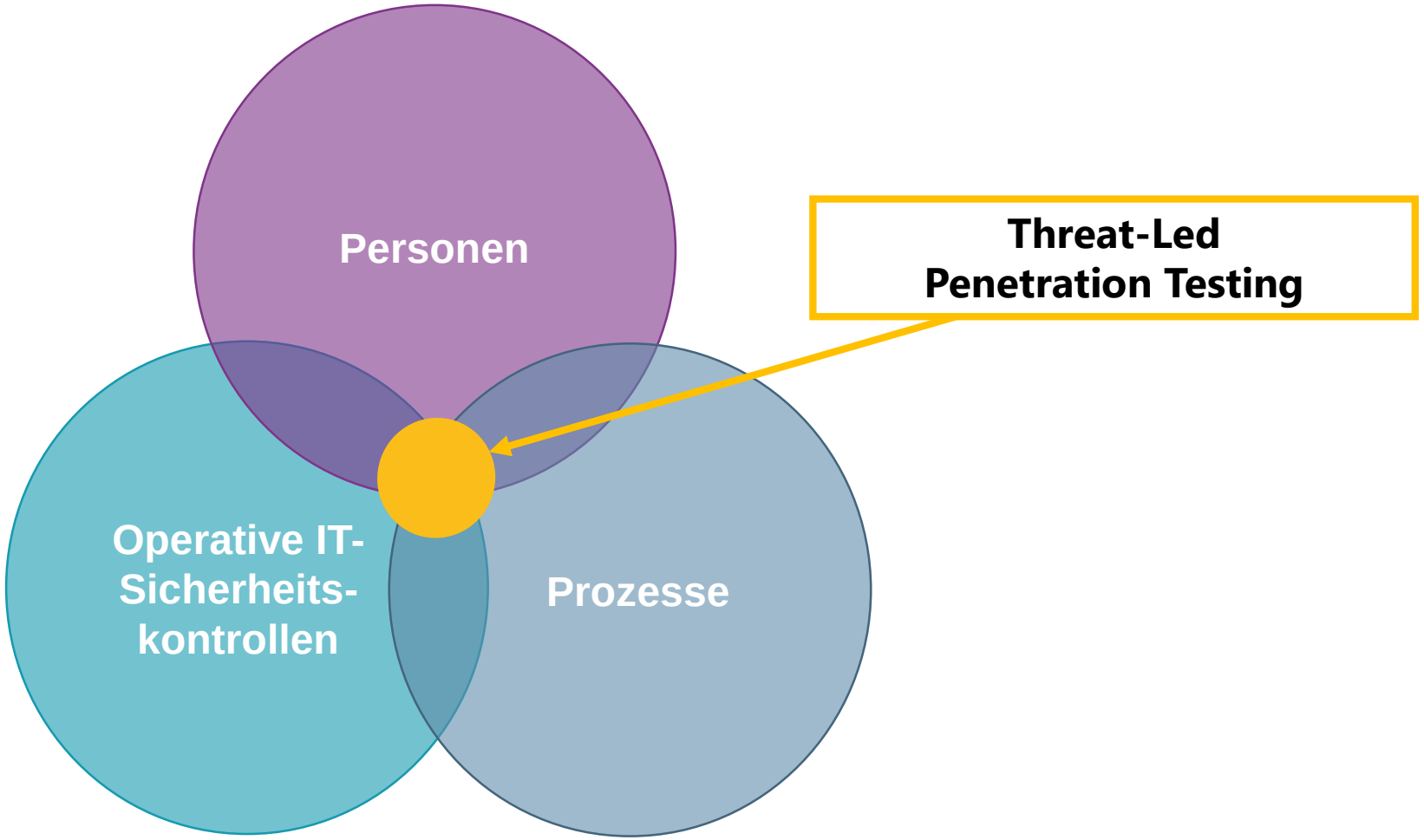
Wofür steht die Abkürzung TLPT in DORA?

Threat- **L**ed **P**enetration **T**esting

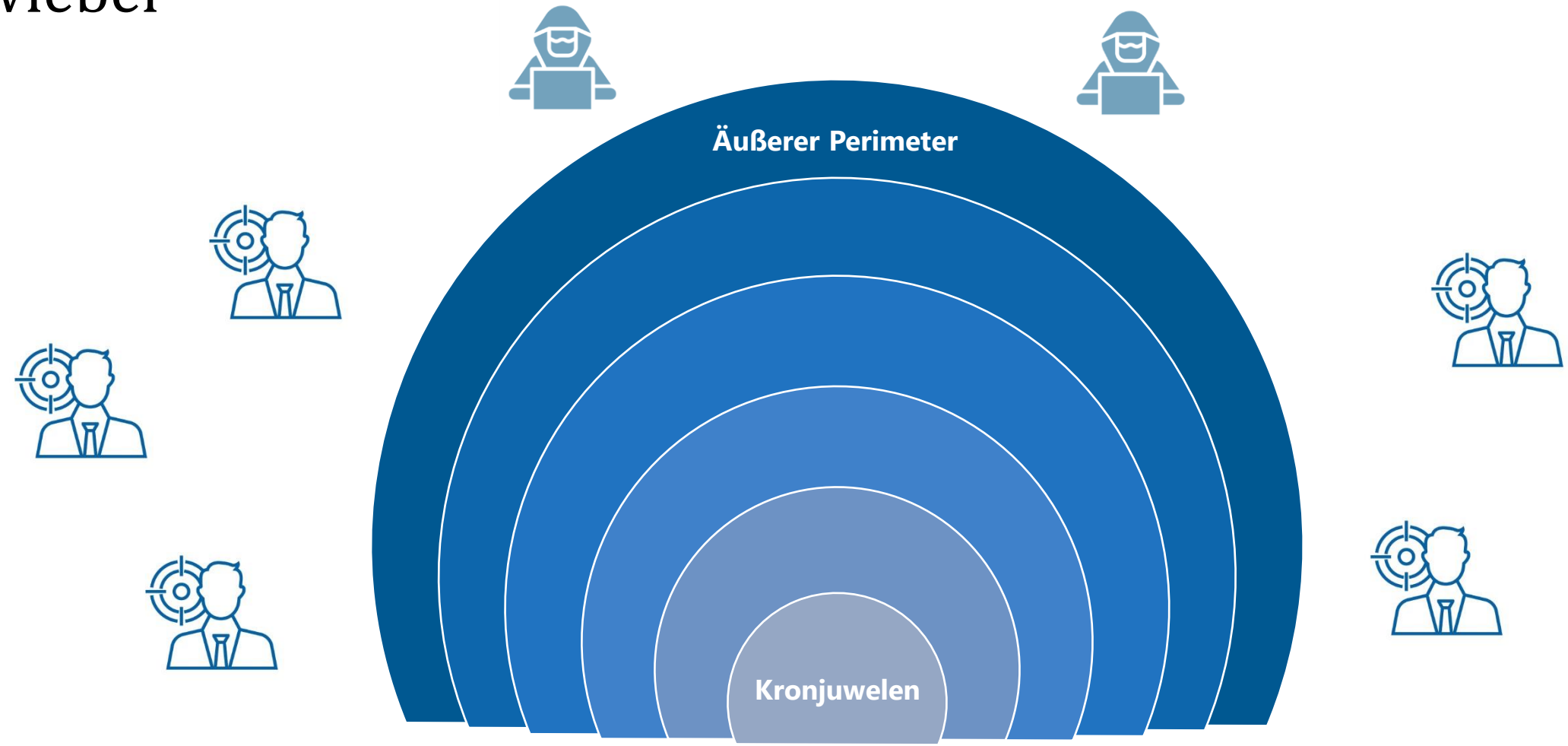
„bedrohungsorientierte Penetrationstests (TLPT – Threat-Led Penetration Testing)“ beschreibt einen Rahmen, der **Taktik, Techniken und Verfahren realer Angreifer**, die als echte Cyberbedrohung empfunden werden, **nachbildet** und einen **kontrollierten**, maßgeschneiderten, erkenntnisgestützten **(Red-Team-) Test** der kritischen **Live-Produktionssysteme** des Finanzunternehmens ermöglicht“*

*Quelle: DORA, Art. 3 (17) Definitionen

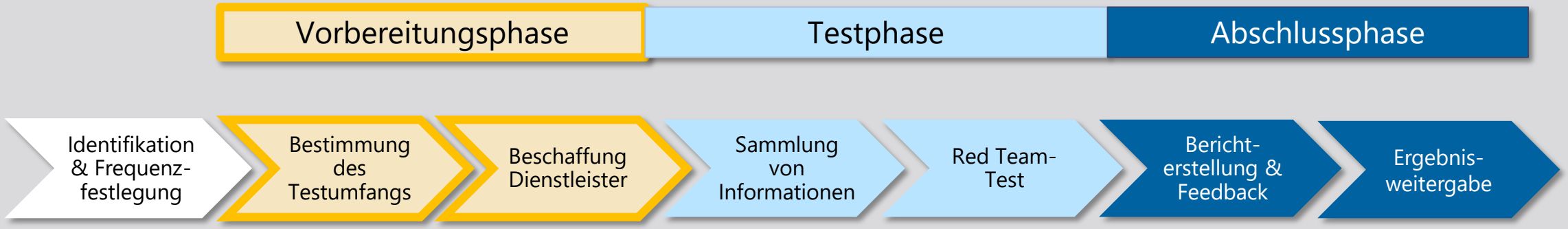
Welchen Mehrwert stiftet Threat-Led Penetration Testing?



Alle Verteidigungslinien werden getestet – „Wir schälen die Zwiebel“



In der Vorbereitungsphase wird die Basis für einen erfolgreichen TLPT gelegt



Die Testmethodik sieht in der Testphase die Einbindung diverser Stakeholder vor

Getestetes Unternehmen

TLPT Cyber Team – Gutachter

TIBER-DE

- Bestätigt die regelkonforme Testdurchführung
- Fachliche und prozessuale Betreuung
- Ansprechpartner für das Control Team
- Hält Kontakt zu externen Stellen

Control Team - Manager

- Zentraler Ansprechpartner und Entscheidungsträger
- Monitoring und Risikomanagement

Threat Intelligence-Anbieter - Spion

- Sammelt unternehmens-spezifische Bedrohungs-informationen
- Erstellt Angriffsszenarien

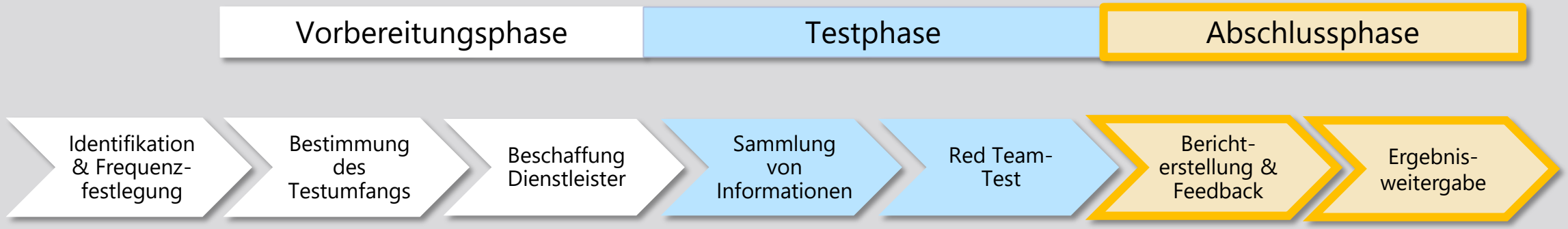
Tester- Angreifer

- Führt Angriffsszenarien auf das Unternehmen durch
- nutzt durch den TI-Anbieter gesammelte Informationen

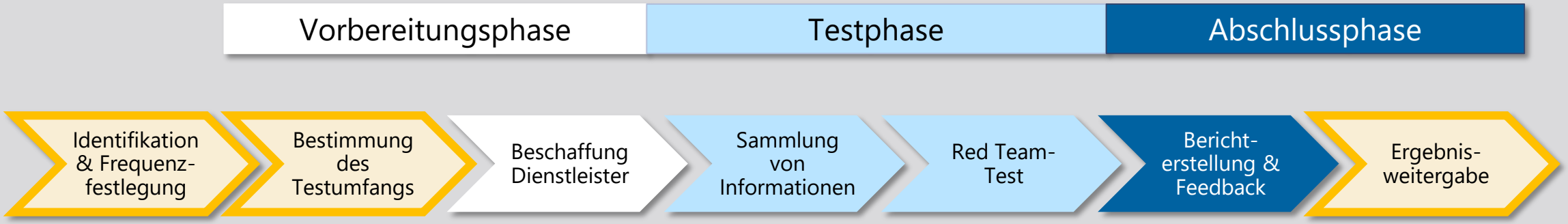
Blue Team - Verteidiger

- Cyberabwehr (SOC/CERT)
- Alle Mitarbeiter außerhalb des Control Teams
- Nicht über die Durchführung des Tests informiert

In der Abschlussphase werden die Ergebnisse analysiert und konkrete Maßnahmen zur Stärkung der Cyberresilienz definiert



Aufgabenteilung für TLPT in Deutschland bleibt im Vergleich zum etablierten Vorgehen unter TIBER-DE nahezu identisch

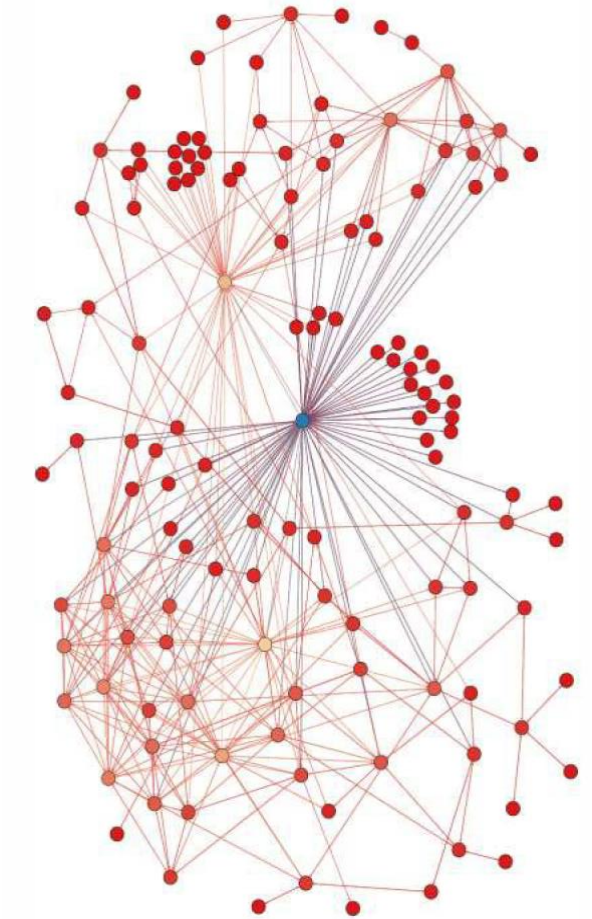


Die zuständige **Finanzaufsicht** identifiziert Finanzunternehmen, die einen TLPT durchführen müssen und legt die Testfrequenz fest.

Die zuständige **Finanzaufsicht** validiert den Testumfang.

Das Unternehmen sendet den Abschlussbericht und den Behebungsplan an die zuständige **Finanzaufsicht**.

Wer muss TLPT ab 2025 durchführen?



Die zuständigen Behörden identifizieren Finanzunternehmen unter Berücksichtigung des **Proportionalitätsprinzips** und der folgenden Kriterien:

a) **wirkungsbezogene Faktoren**, darunter insbesondere inwieweit sich die vom Finanzunternehmen erbrachten Dienstleistungen und Tätigkeiten auf den Finanzsektor auswirken;

b) Bedenken hinsichtlich der **Finanzstabilität**, einschließlich des systemischen Charakters;

c) das **Risikoprofil**, der **IKT-Reifegrad** des Finanzunternehmens oder einschlägige **technologische Merkmale**.

- **Spezifikation** der Kriterien erfolgt im technischen Regulierungsstandard zu TLPT (Art. 26(11) DORA) - Konsultation ab Dezember 2023 geplant
- BaFin wird betroffene Finanzunternehmen von ihrer Verpflichtung informieren

Ganz konkret: Was ändert sich im Vergleich zu TIBER-DE?

Verpflichtung zur Durchführung als **aufsichtliche Maßnahme** für identifizierte Finanzunternehmen

Kleinere **Details** in der **operativen Durchführung** eines TLPT im Vergleich zu dem etablierten TIBER-DE-Rahmenwerk

Interne Tester sind unter besonderen Umständen zugelassen

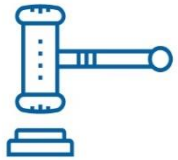
EU-weite Anerkennung von Testergebnissen

Am Ende wird alles gut …

Wie geht es weiter und wo finde ich weiterführende Informationen?

Konsultationsfassung des technischen Regulierungs-standards (RTS) zu TLPT

LINK …wird folgen



Kommentierungsmöglichkeit der öffentlichen Konsultationsfassung des RTS zu TLPT

An wen kann ich mich mit konkreten Fragen wenden?

Informationsveranstaltung zur Konsultationsfassung am 10. Januar 2024

Das TCT der Deutschen Bundesbank und das Referat GIT 1 stehen für Fragen gerne zur Verfügung:

TIBER@Bundesbank.de

GIT1@bafin.de

Vielen Dank für Ihre Aufmerksamkeit!