Prof. Dr. Andreas Igl
TH Deggendorf

Prüfungsplan für den Leiter der Internen Revision: DORA-Prüfungen über drei Jahre

Notiz | April 2025

Dieser Prüfungsplan richtet sich an den **Leiter der Internen Revision** eines Kreditinstituts. Ziel ist es, die Anforderungen des Digital Operational Resilience Act (DORA) in einem **dreijährigen Zyklus mit steigendem Detaillierungsgrad risikoorientiert zu prüfen**. Die Prüfungsgebiete decken verschiedene Themenbereiche ab und bauen aufeinander auf: Im ersten Jahr liegt der Fokus auf grundlegenden Strukturen und Prozessen (Basisprüfung), im zweiten Jahr auf Vertiefung und Schnittstellen (mittlerer Detaillierungsgrad), und im dritten Jahr auf detaillierte Analysen und Optimierungspotenziale (hoher Detaillierungsgrad). Die Ergebnisse dienen als Informationsgrundlage für Vorstände und Aufsichtsräte.

Jahr 1 (2025): Basisprüfung – Grundstrukturen und Compliance

Fokus: Einführung und grundlegende Einhaltung der DORA-Anforderungen
Zeitraum: April 2025 – Dezember 2025

1. **IKT-Risikomanagementrahmen**
    - Prüfungsziel: Verständnis der grundlegenden Struktur und Integration in das übergeordnete Risikomanagement.
    - Fragen: Wie wird das IKT-Risikomanagement in den übergeordneten Risikomanagementrahmen integriert? Welche Methoden zur Risikoidentifikation gibt es?
    - Umfang: Überblick über Prozesse, Dokumentationen und Verantwortlichkeiten.
2. **Klassifikation von kritischen oder wichtigen Funktionen**
    - Prüfungsziel: Sicherstellung einer konsistenten Klassifikation und Dokumentation.
    - Fragen: Wie wird die Wesentlichkeit kritischer Funktionen definiert? Welche Prozesse klassifizieren kritische Funktionen?

- Umfang: Überprüfung der Klassifikationskriterien und -dokumentation.

3. **IT- und DORA-Strategieprozess**
   - Prüfungsziel: Grundlegende Verzahnung mit der Geschäftsstrategie.
   - Fragen: Wie ist die IT-Strategie mit der Geschäftsstrategie verknüpft? Wie oft wird die Strategie überprüft?
   - Umfang: Analyse der Strategiedokumente und Überprüfungszyklen.
4. **IKT-Kontrollfunktion und Schnittstelle zum ISB**
   - Prüfungsziel: Klärung der Zuständigkeiten und Berichtslinien.
   - Fragen: Wie sind die Zuständigkeiten der IKT-Kontrollfunktion definiert? Wie ist die Zusammenarbeit mit dem ISB organisiert?
   - Umfang: Überblick über Organisationsstruktur und Berichtswesen.
5. **IKT-Drittparteirisikomanagement**
   - Prüfungsziel: Grundlegende Identifikation und Vertragsgestaltung.
   - Fragen: Wie werden kritische IKT-Dienstleister identifiziert? Welche DORA-Anforderungen sind in Verträgen enthalten?
   - Umfang: Stichproben von Verträgen und Risikobewertungen.

Jahr 2 (2026): Vertiefung – Schnittstellen und Prozessqualität

Fokus: Vertiefung der Prüfungen mit Blick auf Schnittstellen und Wirksamkeit
Zeitraum: Januar 2026 – Dezember 2026

1. **IKT-Risikomanagementrahmen**
   - Prüfungsziel: Vertiefte Analyse von Risikosteuerung und Monitoring.
   - Fragen: Welche Maßnahmen zur Risikominderung wurden implementiert? Welche Instrumente überwachen IKT-Risiken?
   - Umfang: Prüfung der Wirksamkeit von Kontrollen und Monitoring-Tools.
2. **Klassifikation von kritischen oder wichtigen Funktionen**
   - Prüfungsziel: Überprüfung der Verzahnung mit Auslagerungsmanagement und Notfallplänen.

- Fragen: Wie wird die Klassifikation mit dem Auslagerungsmanagement abgestimmt? Wie wird die Kritikalität im Notfall bewertet (BIA)?
- Umfang: Analyse von Schnittstellen und Business Impact Analysen.

3. **IT- und DORA-Strategieprozess**
   - Prüfungsziel: Integration in die Risikostrategie und Krisenmanagement.
   - Fragen: Wie werden IKT-Risiken in die Risikostrategie integriert? Welche Notfallpläne gibt es für IKT-Vorfälle?
   - Umfang: Prüfung der Krisenpläne und Risikostrategie-Dokumentation.
4. **IKT-Geschäftsfortführungsmanagement (Leitlinie und Pläne)**
   - Prüfungsziel: Integration und Szenarien der Geschäftsfortführung.
   - Fragen: Wie ist die IKT-Leitlinie in das bankweite BCM eingebunden? Welche Szenarien sind in den Wiederherstellungsplänen abgedeckt?
   - Umfang: Überprüfung der Leitlinie und Stichproben von Plänen.
5. **DORA-Meldeverpflichtungen**
   - Prüfungsziel: Funktionsweise der Meldeprozesse und Informationsregister.
   - Fragen: Wie wird ein schwerwiegender IKT-Vorfall identifiziert? Wie wird das Informationsregister verwaltet?
   - Umfang: Test des Meldeprozesses und Registerprüfung.

Jahr 3 (2027): Detaillierte Analyse – Optimierung und Resilienz

Fokus: Detaillierte Prüfung auf Optimierungspotenziale und Resilienz
Zeitraum: Januar 2027 – Dezember 2027

1. **IKT-Risikomanagementrahmen**
   - Prüfungsziel: Detaillierte Analyse von Notfallmanagement und ICAAP-Verzahnung.
   - Fragen: Welche Notfallpläne gibt es für IKT-Risiken? Wie fließen IKT-Risiken in den ICAAP ein?

- Umfang: Tiefgehende Analyse von Notfallplänen und Kapitalberechnungen.

2. **IKT-Drittparteirisikomanagement und Auslagerungsmanagement**
   - Prüfungsziel: Detaillierte Prüfung der Vertragslebenszyklen und Kontrollen.
   - Fragen: Wie wird der Vertragslebenszyklus gesteuert? Wie sind Drittparteirisiken mit dem Auslagerungsmanagement abgestimmt?
   - Umfang: Prüfung des gesamten Zyklus und der Governance-Strukturen.
3. **IKT-Geschäftsfortführungsmanagement (Leitlinie und Pläne)**
   - Prüfungsziel: Testen und Optimierung der Pläne.
   - Fragen: Wie werden Wiederherstellungspläne getestet? Welche Schulungen gibt es für Notfälle?
   - Umfang: Analyse von Testergebnissen und Schulungsprotokollen.
4. **DORA-Meldeverpflichtungen**
   - Prüfungsziel: Qualitätssicherung und Nachverfolgung.
   - Fragen: Wie wird die Qualität der Meldungen überprüft? Wie wird auf Rückmeldungen der Behörden reagiert?
   - Umfang: Detaillierte Analyse von Berichten und Nachverfolgungsprozessen.
5. **Aufbau von IT-Kompetenz in der Revision**
   - Prüfungsziel: Bewertung der Kompetenzentwicklung und ihrer Wirkung.
   - Fragen: Welche Schulungen wurden besucht und wie wird die Kompetenz überprüft? Wie unterstützt das Kompetenznetzwerk die Prüfungen?
   - Umfang: Evaluierung von Schulungsmaßnahmen und deren Einfluss auf Prüfungsqualität.

Zusammenfassung des Prüfungsplans

- **Jahr 1 (2025):** Grundlegende Strukturen und Prozesse werden geprüft, um die DORA-Compliance sicherzustellen (z. B. IKT-Risikomanagementrahmen, Klassifikation kritischer Funktionen).

- **Jahr 2 (2026):** Vertiefung der Prüfungen mit Fokus auf Schnittstellen, Wirksamkeit und Prozessqualität (z. B. IKT-Geschäftsfortführung, Meldeverpflichtungen).
- **Jahr 3 (2027):** Detaillierte Analyse mit Blick auf Optimierung, Resilienz und Kompetenzentwicklung (z. B. Notfallmanagement, Vertragslebenszyklus, IT-Kompetenz).

Empfehlungen für die Umsetzung

- **Ressourcen:** Sicherstellung ausreichender Kapazitäten und IT-Kompetenz in der Revision (siehe Schulungsformate).
- **Dokumentation:** Jährliche Berichte mit Handlungsempfehlungen für Vorstand und Aufsichtsrat.
- **Flexibilität:** Anpassung des Plans bei regulatorischen Änderungen oder schwerwiegenden IKT-Vorfällen.

Dieser Plan ermöglicht eine systematische und risikoorientierte Prüfung, die den Anforderungen der dritten Verteidigungslinie gerecht wird und die digitale Resilienz des Instituts nachhaltig stärkt.

Prof. Dr. Andreas Igl
BDO-Stiftungsprofessor an der TH Deggendorf
Lehrbeauftragter an der Hochschule der Deutschen Bundesbank

andreas.igl@th-deg.de
(Mobil): 0151 2301 8610
(LinkedIn): Link