Arbeitsanweisung für die Funktion Risikomanagement gemäß DORA

Generiert am: 28.05.2025

# Ziel

Ziel dieser Arbeitsanweisung ist es, die Aufgaben und Verantwortlichkeiten der Funktion Risikomanagement im Kontext der Verordnung (EU) 2022/2554 (DORA) und der dazugehörigen technischen Regulierungsstandards (RTS/ITS) klar zu definieren. Es soll sichergestellt werden, dass die Bank die regulatorischen Anforderungen an die digitale operationale Resilienz erfüllt.

*Dabei ist dem Grundsatz der Verhältnismäßigkeit gemäß Artikel 4 VO (EU) 2022/2554 Rechnung zu tragen, der die Größe, das Gesamtrisikoprofil sowie die Art, den Umfang und die Komplexität der Dienstleistungen, Tätigkeiten und Geschäfte der Bank berücksichtigt.*

# 1. Aufgaben im Bereich der direkten Verantwortung

## 1.1. IKT-Risikomanagementrahmen und Governance:

* Entwicklung, Implementierung, Dokumentation und regelmäßige Überprüfung eines umfassenden, schriftlich fixierten IKT-Risikomanagementrahmens. Dieser Rahmen enthält Strategien, Richtlinien, Verfahren und Kontrollmechanismen für IKT-Risiken und muss Vollständigkeit und Aktualität gewährleisten.
* Mindestens jährliche Aktualisierung des IKT-Risikomanagementrahmens oder bei Auftreten schwerwiegender IKT-bezogener Vorfälle sowie nach aufsichtlichen Anweisungen oder Feststellungen aus Tests oder Audits. Kontinuierliche Verbesserung auf Basis gewonnener Erkenntnisse.
* Evaluierung und Anpassung des IKT-Risikomanagementrahmens nach Vorfällen, insbesondere wenn Defizite erkennbar werden.
* Implementierung einer wirkungsvollen Governance-Struktur und Organisationsform, die das Management von IKT-Risiken effektiv unterstützt.
* Sicherstellung, dass das Leitungsorgan über ausreichende Kenntnisse und Fähigkeiten zur Bewertung von IKT-Risiken verfügt und regelmäßige, bedarfsgerechte Schulungen erhält.
* Etablierung einer Funktion zur Überwachung des IKT-Risikos mit angemessener Unabhängigkeit (Kontrollfunktion), um Interessenkonflikte zu vermeiden und eine angemessene Trennung von IKT-Risikomanagementfunktionen, Kontrollfunktionen und internen Revisionsfunktionen sicherzustellen.
* Festlegung klarer Aufgaben und Verantwortlichkeiten für alle IKT-bezogenen Funktionen und Sicherstellung angemessener Governance-Regelungen für eine wirksame Kommunikation und Koordination.
* Dokumentation und Archivierung aller DORA-relevanten Prozesse, um eine nachweisbare Dokumentation für interne und externe Prüfungen sicherzustellen.

*Quelle(n): VO (EU) 2022/2554, Art. 5(1); VO (EU) 2022/2554, Art. 5(2); VO (EU) 2022/2554, Art. 5(4); VO (EU) 2022/2554, Art. 6(1); VO (EU) 2022/2554, Art. 6(2); VO (EU) 2022/2554, Art. 6(3); VO (EU) 2022/2554, Art. 6(4); VO (EU) 2022/2554, Art. 6(5); VO (EU) 2022/2554, Art. 6(8); VO (EU) 2022/2554, Art. 13(2); VO (EU) 2022/2554, Art. 13(3)*

## 1.2. Management von IKT-Drittparteienrisiken:

* Festlegung und Anwendung eines angemessenen und verhältnismäßigen Verfahrens zur Sorgfaltspflicht bei der Auswahl und Bewertung von IKT-Drittdienstleistern, unter Beachtung von deren Reputation, Fähigkeiten, Ressourcen, Informationssicherheitsstandards und ethischem Verhalten.
* Sicherstellung der vollen Kontrolle über die Risiken, die von IKT-Drittdienstleistungen ausgehen, einschließlich der Risiken durch Unterauftragnehmer.
* Durchführung einer Ex-ante-Risikobewertung vor Vertragsabschluss mit IKT-Drittdienstleistern, die operationelle, rechtliche, IKT- und Reputationsrisiken sowie Risiken bezüglich Datenschutz, Datenverfügbarkeit, Standort und Konzentration berücksichtigt.
* Angemessene Bewertung und Steuerung von Drittparteienrisiken.
* Führung und Aktualisierung eines Informationsregisters über alle vertraglichen Vereinbarungen mit IKT-Drittdienstleistern, inklusive regelmäßiger Vertragsprüfung zur Sicherstellung vollständiger und gesetzeskonformer Verträge.
* Harmonisierte Einbindung von Drittparteienrisiken in das gesamte IKT-Risikomanagement.

*Quelle(n): VO (EU) 2022/2554, Art. 28(1); VO (EU) 2022/2554, Art. 28(2); VO (EU) 2022/2554, Art. 28(3); VO (EU) 2022/2554, Art. 28(4); VO (EU) 2022/2554, Art. 28(5); VO (EU) 2022/2554, Art. 28(6); VO (EU) 2022/2554, Art. 28(7); VO (EU) 2022/2554, Art. 28(8); VO (EU) 2022/2554, Art. 29(1); VO (EU) 2022/2554, Art. 29(2); VO (EU) 2022/2554, Art. 30(1); VO (EU) 2022/2554, Art. 30(2); VO (EU) 2022/2554, Art. 30(3); VO (EU) 2024/1773, Art. 5(1); VO (EU) 2024/1773, Art. 5(2); VO (EU) 2024/1773, Art. 6(1); VO (EU) 2024/1773, Art. 6(2); VO (EU) 2024/1773, Art. 6(3); VO (EU) 2024/1773, Art. 6(4)*

## 1.3. Identifizierung, Klassifizierung und Schutz von IKT-Assets und -Systemen:

* Erstellung, Pflege und regelmäßige Überprüfung eines vollständigen IKT-Asset-Registers, das alle IKT-gestützten Unternehmensfunktionen, Informations- und IKT-Assets (inkl. Standort, Besitzer) sowie deren Konfigurationen, Verbindungen und Abhängigkeiten dokumentiert und klassifiziert.
* Durchführung einer Kritikalitätsbewertung von Informationsassets und IKT-Assets basierend auf deren Bedeutung für Unternehmensfunktionen und den potenziellen Auswirkungen bei Verlust von Vertraulichkeit, Integrität oder Verfügbarkeit. Diese Bewertung dient als Grundlage für Schutzmaßnahmen.
* Überwachung des Lebenszyklus von IKT-Systemen mit besonderem Fokus auf Altsysteme und Durchführung spezifischer Risikobewertungen für diese.
* Erarbeitung und Dokumentation einer Informationssicherheitsleitlinie, die vom Leitungsorgan zu verabschieden ist und Regeln zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten und IKT-Assets festlegt.
* Implementierung einer Richtlinie für Verschlüsselung und kryptografische Kontrollen, die auf Datenklassifizierung und IKT-Risikobewertung basiert und das Management kryptografischer Schlüssel über deren gesamten Lebenszyklus regelt.
* Sicherstellung des Schutzes von Informationen bei der Übermittlung intern und extern, basierend auf Datenklassifizierung und Risikobewertung, einschließlich Maßnahmen zur Verhinderung und Erkennung von Datenlecks.
* Definition und Dokumentation aller IKT-Vorgänge, einschließlich der Trennung von Produktions-, Entwicklungs- und Testumgebungen, um Störungen zu vermeiden und klare Vorgaben für Notfälle und Fehlerbehandlung zu schaffen.
* Überwachung und Optimierung von IKT-Kapazitäten und -Leistung zur Ermittlung von Anforderungen, Anwendung von Ressourcenoptimierungsmethoden und Verhinderung von Kapazitätsengpässen, insbesondere bei kritischen Systemen.
* Implementierung und Dokumentation von Richtlinien, Verfahren und Kontrollen für das IKT-Änderungsmanagement, die auf einem Risikobewertungsansatz basieren und sicherstellen, dass alle Änderungen kontrolliert erfasst, getestet, bewertet, genehmigt, implementiert und überprüft werden. Dies umfasst Aufgabentrennung, Rückfallpläne und Testverfahren.

*Quelle(n): VO (EU) 2022/2554, Art. 7; VO (EU) 2022/2554, Art. 8(1); VO (EU) 2022/2554, Art. 8(2); VO (EU) 2022/2554, Art. 8(4); VO (EU) 2022/2554, Art. 8(5); VO (EU) 2022/2554, Art. 8(6); VO (EU) 2022/2554, Art. 8(7); VO (EU) 2022/2554, Art. 9(1); VO (EU) 2022/2554, Art. 9(2); VO (EU) 2022/2554, Art. 9(3); VO (EU) 2022/2554, Art. 9(4); VO (EU) 2024/1774, Art. 4(1); VO (EU) 2024/1774, Art. 4(2); VO (EU) 2024/1774, Art. 5(1); VO (EU) 2024/1774, Art. 5(2); VO (EU) 2024/1774, Art. 6(1); VO (EU) 2024/1774, Art. 6(2); VO (EU) 2024/1774, Art. 6(3); VO (EU) 2024/1774, Art. 6(4); VO (EU) 2024/1774, Art. 6(5); VO (EU) 2024/1774, Art. 7(1); VO (EU) 2024/1774, Art. 7(2); VO (EU) 2024/1774, Art. 7(3); VO (EU) 2024/1774, Art. 7(4); VO (EU) 2024/1774, Art. 7(5); VO (EU) 2024/1774, Art. 8(1); VO (EU) 2024/1774, Art. 8(2); VO (EU) 2024/1774, Art. 9(1); VO (EU) 2024/1774, Art. 9(2); VO (EU) 2024/1774, Art. 14(1); VO (EU) 2024/1774, Art. 14(2); VO (EU) 2024/1774, Art. 17(1); VO (EU) 2024/1774, Art. 20(1); VO (EU) 2024/1774, Art. 20(2); VO (EU) 2024/1774, Art. 21*

## 1.4. Management von IKT-bezogenen Vorfällen und Schwachstellen:

* Entwicklung, Dokumentation und Implementierung von Verfahren, Protokollen und Tools für die Datenaufzeichnung (Protokollierung). Dies beinhaltet die Ermittlung aufzuzeichnender Ereignisse, Festlegung von Speicherfristen und Maßnahmen zur Sicherung, Verarbeitung und zum Schutz der Aufzeichnungsdaten vor Manipulation, Löschung und unbefugtem Zugriff sowie die Synchronisierung der Uhren.
* Kontinuierliche Sammlung von Informationen über Schwachstellen und Cyberbedrohungen sowie deren wahrscheinliche Auswirkungen auf die digitale operationale Resilienz.
* Implementierung von Mechanismen zur umgehenden Erkennung anomaler Aktivitäten, einschließlich automatisierter Alarme für Angriffe oder Abweichungen, die durch spezialisiertes Personal überprüft werden.
* Festlegung und Umsetzung einer Strategie für den Umgang mit IKT-bezogenen Vorfällen, die Prozesse zur Erkennung, zum Management und zur Meldung von IKT-Vorfällen sowie zur Analyse der Ursachen und zur Festlegung von Verantwortlichkeiten umfasst.
* Definition und Implementierung sofortiger Eindämmungsmaßnahmen und angepasster Verfahren zur Begrenzung von Schäden und Vermeidung weiterer Auswirkungen im Falle von IKT-Vorfällen.
* Entwicklung und Umsetzung von Kommunikationsstrategien für die Unterrichtung von internen Mitarbeitern, externen Interessenträgern und gegebenenfalls Behörden über schwerwiegende IKT-bezogene Vorfälle.

*Quelle(n): VO (EU) 2022/2554, Art. 10(1); VO (EU) 2022/2554, Art. 10(2); VO (EU) 2022/2554, Art. 10(3); VO (EU) 2022/2554, Art. 11(1); VO (EU) 2022/2554, Art. 11(2); VO (EU) 2022/2554, Art. 13(1); VO (EU) 2022/2554, Art. 14; VO (EU) 2024/1774, Art. 12(1); VO (EU) 2024/1774, Art. 12(2)*

## 1.5. Tests der digitalen operationalen Resilienz und IKT-Projektmanagement:

* Durchführung einer mindestens jährlichen Risikobewertung und Neubewertung von IKT-Systemen, insbesondere bei jeder wesentlichen Änderung oder Integration neuer Systeme.
* Regelmäßige Durchführung unabhängiger Tests der Schutzmaßnahmen und des Schwachstellenmanagements.
* Entwicklung, Dokumentation und Implementierung von Richtlinien für das IKT-Projektmanagement, die Ziele, Governance, Planung, Risikobewertung, Etappenziele, Änderungsmanagement und Testanforderungen (einschließlich Sicherheitsanforderungen) für IKT-Projekte festlegen. Sicherstellung der Einbindung betroffener Fachbereiche und der Berichterstattung an das Leitungsorgan.
* Durchführung angemessener Tests der digitalen operationalen Resilienz gemäß Kapitel IV der VO (EU) 2022/2554, die dem Risikoprofil und der Größe der Bank entsprechen. Für eine kleine Bank bedeutet dies in der Regel grundlegende und erweiterte Tests, einschließlich Schwachstellenbewertungen und Szenario-basierte Tests. Die Notwendigkeit für Threat-Led Penetration Tests (TLPT) ist gesondert zu prüfen und von der zuständigen Behörde abhängig.

*Quelle(n): VO (EU) 2022/2554, Art. 6(8)g; VO (EU) 2022/2554, Art. 8(3); VO (EU) 2022/2554, Art. 8(7); VO (EU) 2022/2554, Art. 24; VO (EU) 2022/2554, Art. 25; VO (EU) 2024/1774, Art. 15(1); VO (EU) 2024/1774, Art. 15(2); VO (EU) 2024/1774, Art. 15(3); VO (EU) 2024/1774, Art. 15(4); VO (EU) 2024/1774, Art. 15(5)*

*Hinweis: Die Verpflichtung zu Threat-Led Penetration Tests (TLPT) gemäß Art. 26 VO (EU) 2022/2554 gilt nicht automatisch für alle Finanzunternehmen. Für eine kleine Bank ist dies nur relevant, wenn sie von der zuständigen Behörde explizit dazu aufgefordert wird.*

## 1.6. Sicherstellung angemessener Ressourcen und Berichtswege:

Sicherstellung der Bereitstellung angemessener Ressourcen (finanziell, personell, technisch) und klarer Berichtswege für das Management und die Überwachung von IKT-Risiken.

*Quelle(n): VO (EU) 2022/2554, Art. 5(2)g; VO (EU) 2022/2554, Art. 6(4)*

# 2. Aufgaben im Bereich der Mitwirkungspflicht

## 2.1. IKT-Risikomanagementrahmen und Governance (Mitwirkung):

* Mitwirkung bei der regelmäßigen Überprüfung und Aktualisierung des IKT-Risikomanagementrahmens, mindestens jährlich oder bei Vorfällen, sowie nach aufsichtlichen Feststellungen oder Ergebnissen aus Tests und Audits.
* Unterstützung bei der Dokumentation und Archivierung aller DORA-relevanten Prozesse zur Sicherstellung der Nachweisbarkeit für interne und externe Prüfungen.
* Unterstützung der unabhängigen IKT-Kontrollfunktion bei der Überwachung von IKT-Risiken durch Bereitstellung von Informationen und Analysen.
* Mitwirkung bei der Erstellung, Dokumentation und Überprüfung der Informationssicherheitsleitlinie zum Schutz der Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit.
* Mitwirkung bei der Entwicklung von Richtlinien für das IKT-Projektmanagement, insbesondere bei der Risikobewertung von Projekten und der Definition von Testmethoden.

*Quelle(n): VO (EU) 2022/2554, Art. 5(1); VO (EU) 2022/2554, Art. 5(2); VO (EU) 2022/2554, Art. 6(1); VO (EU) 2022/2554, Art. 6(4); VO (EU) 2022/2554, Art. 6(5); VO (EU) 2022/2554, Art. 9(4)a; VO (EU) 2024/1774, Art. 15(1); VO (EU) 2024/1774, Art. 15(2); VO (EU) 2024/1774, Art. 15(3); VO (EU) 2024/1774, Art. 15(4); VO (EU) 2024/1774, Art. 15(5)*

## 2.2. Management von IKT-Drittparteienrisiken (Mitwirkung):

* Unterstützung bei der Durchführung der Sorgfaltspflicht bei der Auswahl und Bewertung von IKT-Dienstleistern durch Risikobewertungen und Analyse der Dienstleisterinformationen.
* Mitwirkung bei der Entwicklung, Pflege und regelmäßigen Überprüfung und Testung von Ausstiegsplänen für vertragliche Vereinbarungen mit IKT-Drittdienstleistern, die realistische Szenarien für Unterbrechungen, Vertragsverletzungen und Exit-Szenarien berücksichtigen.
* Unterstützung bei der Überwachung und Kontrolle von Drittparteienrisiken, einschließlich der Risiken von Unterauftragnehmern, durch Bereitstellung von Risikoanalysen.
* Mitwirkung bei der Sicherstellung, dass vertragliche Vereinbarungen mit IKT-Drittdienstleistern mit dem IKT-Risikomanagementrahmen, der Informationssicherheitsleitlinie und der IKT-Geschäftsfortführungsleitlinie im Einklang stehen.
* Unterstützung bei der Führung und Aktualisierung des Informationsregisters über alle Verträge mit IKT-Drittdienstleistern, insbesondere durch die Identifizierung und Bewertung von Risiken.
* Mitwirkung beim kontinuierlichen Monitoring der Leistung von IKT-Drittdienstleistern, einschließlich der Überprüfung von KPIs, Berichten und Audits, und Unterstützung bei Eskalationsprozessen.
* Mitwirkung bei der Definition von Mindestvertragsinhalten für Vereinbarungen mit IKT-Drittdienstleistern, insbesondere hinsichtlich Audit- und Zugangsrechten sowie Sicherheitsanforderungen.
* Unterstützung bei der Sicherstellung, dass Verträge mit IKT-Dienstleistern umfassend sind und alle aufsichtsrechtlichen Anforderungen erfüllen.

*Quelle(n): VO (EU) 2022/2554, Art. 28(1); VO (EU) 2022/2554, Art. 28(2); VO (EU) 2022/2554, Art. 28(3); VO (EU) 2022/2554, Art. 28(4); VO (EU) 2022/2554, Art. 28(8); VO (EU) 2022/2554, Art. 30(1); VO (EU) 2022/2554, Art. 30(2); VO (EU) 2022/2554, Art. 30(3); VO (EU) 2024/1773, Art. 3(6); VO (EU) 2024/1773, Art. 6(1); VO (EU) 2024/1773, Art. 6(2); VO (EU) 2024/1773, Art. 6(3); VO (EU) 2024/1773, Art. 6(4); VO (EU) 2024/1773, Art. 8(1); VO (EU) 2024/1773, Art. 8(2); VO (EU) 2024/1773, Art. 8(3); VO (EU) 2024/1773, Art. 8(4); VO (EU) 2024/1773, Art. 9(1); VO (EU) 2024/1773, Art. 9(2); VO (EU) 2024/1773, Art. 9(3); VO (EU) 2024/1773, Art. 9(4); VO (EU) 2024/1773, Art. 10*

## 2.3. IKT-Sicherheitsmaßnahmen und Schutz (Mitwirkung):

* Mitwirkung bei der Überwachung und Optimierung von IKT-Kapazitäten und -Leistung durch Analyse von Leistungsdaten und Risikobewertungen.
* Unterstützung bei der Definition der aufzuzeichnenden Ereignisse, Speicherfristen und Schutzmaßnahmen für Protokolldaten aus Risikomanagementsicht.
* Mitwirkung bei der Definition und Dokumentation aller IKT-Vorgänge, insbesondere hinsichtlich der Risikominimierung durch Trennung von Produktions- und Testumgebungen.
* Mitwirkung bei der Erstellung und Überprüfung von Richtlinien für sichere Konfigurationen, Malware-Abwehr, sichere Nutzung von Geräten (auch bei Telearbeit) und Datenlöschung aus Risikoperspektive.
* Unterstützung bei der Kritikalitätsbewertung von Daten und Systemen durch Bereitstellung von Risikoeinschätzungen.
* Mitwirkung bei der Implementierung und Überprüfung einer Richtlinie für Verschlüsselung und kryptografische Kontrollen unter Berücksichtigung aktueller Risiken.
* Mitwirkung bei der Etablierung und Überprüfung eines Prozesses für Schwachstellen- und Patch-Management, einschließlich der Priorisierung basierend auf Risikobewertungen.
* Unterstützung bei der Dokumentation und Kontrolle aller Änderungen an IKT-Systemen, insbesondere bei der Risikobewertung von Änderungen und der Überprüfung von Rückfallplänen.
* Mitwirkung bei der Konzeption und Überprüfung technisch-organisatorischer Maßnahmen zur Sicherstellung der Arbeitsfähigkeit bei IKT-Vorfällen.
* Mitwirkung beim Schutz von Informationen bei der Übermittlung intern und extern durch Risikobewertung der Übertragungswege und -methoden.

*Quelle(n): VO (EU) 2022/2554, Art. 4(1); VO (EU) 2022/2554, Art. 4(2); VO (EU) 2022/2554, Art. 7; VO (EU) 2022/2554, Art. 9(4)a; VO (EU) 2022/2554, Art. 9(4)e; VO (EU) 2024/1774, Art. 5(1); VO (EU) 2024/1774, Art. 5(2); VO (EU) 2024/1774, Art. 6(1); VO (EU) 2024/1774, Art. 6(2); VO (EU) 2024/1774, Art. 8(1); VO (EU) 2024/1774, Art. 8(2); VO (EU) 2024/1774, Art. 9(1); VO (EU) 2024/1774, Art. 9(2); VO (EU) 2024/1774, Art. 10(1); VO (EU) 2024/1774, Art. 10(2); VO (EU) 2024/1774, Art. 10(3); VO (EU) 2024/1774, Art. 10(4); VO (EU) 2024/1774, Art. 11(1); VO (EU) 2024/1774, Art. 11(2); VO (EU) 2024/1774, Art. 12(1); VO (EU) 2024/1774, Art. 12(2); VO (EU) 2024/1774, Art. 14(1); VO (EU) 2024/1774, Art. 14(2); VO (EU) 2024/1774, Art. 17(1); VO (EU) 2024/1774, Art. 18(1); VO (EU) 2024/1774, Art. 18(2); VO (EU) 2024/1774, Art. 19; VO (EU) 2024/1774, Art. 20(1); VO (EU) 2024/1774, Art. 20(2); VO (EU) 2024/1774, Art. 21*

## 2.4. IKT-Geschäftsfortführungsmanagement und Reaktion auf Vorfälle (Mitwirkung):

* Mitwirkung bei der Entwicklung, Implementierung und Überprüfung effektiver Notfallpläne (IKT-Geschäftsfortführungspläne, IKT-Reaktions- und Wiederherstellungspläne) zur Aufrechterhaltung kritischer Funktionen bei Störungen und zur Begrenzung von Schäden.
* Unterstützung bei der Einrichtung und Überprüfung von Mechanismen zur proaktiven Erkennung anomaler Aktivitäten und potenzieller Schwachstellen.
* Mitwirkung bei der Entwicklung und Überprüfung robuster Backup-Strategien, einschließlich der Festlegung von Backup-Zyklen, Wiederherstellungsmethoden und Tests der Datensicherungssysteme, um den Schutz vor katastrophalen Schäden zu gewährleisten.
* Unterstützung bei der Planung und Durchführung regelmäßiger Tests der Notfallpläne, einschließlich der Entwicklung detaillierter Szenarien (z.B. Cyberangriffe, Umstellungen auf redundante Systeme).
* Mitwirkung bei der Entwicklung und Umsetzung von Kommunikationsstrategien für interne und externe Stakeholder sowie Behörden im Krisenfall.
* Unterstützung bei der Sicherstellung, dass ausreichende Ressourcen und Tools mit klaren Zuständigkeiten für das Management von IKT-Vorfällen und die Geschäftsfortführung vorhanden sind.
* Mitwirkung bei der Festlegung und Überprüfung einer Strategie für IKT-bezogene Vorfälle, die Erkennung, Reaktion, Analyse der Ursachen und Verantwortlichkeiten umfasst.
* Unterstützung bei der Erstellung aufsichtsrechtlicher Berichte über schwerwiegende IKT-bezogene Vorfälle und Koordination der Kommunikation mit Aufsichtsbehörden.

*Quelle(n): VO (EU) 2022/2554, Art. 10(1); VO (EU) 2022/2554, Art. 10(2); VO (EU) 2022/2554, Art. 11(1); VO (EU) 2022/2554, Art. 11(2); VO (EU) 2022/2554, Art. 11(3); VO (EU) 2022/2554, Art. 11(4); VO (EU) 2022/2554, Art. 11(5); VO (EU) 2022/2554, Art. 11(6); VO (EU) 2022/2554, Art. 11(7); VO (EU) 2022/2554, Art. 11(8); VO (EU) 2022/2554, Art. 12(1); VO (EU) 2022/2554, Art. 12(2); VO (EU) 2022/2554, Art. 12(3); VO (EU) 2022/2554, Art. 14; VO (EU) 2022/2554, Art. 19(1); VO (EU) 2022/2554, Art. 19(2); VO (EU) 2022/2554, Art. 19(3); VO (EU) 2022/2554, Art. 19(4)*

## 2.5. Tests der digitalen operationalen Resilienz und Informationsaustausch (Mitwirkung):

* Mitwirkung bei der Planung, Koordination und Durchführung von Tests der digitalen operationalen Resilienz, einschließlich Penetrationstests, die dem Risikoprofil und der Größe der Bank angemessen sind. Unterstützung bei der Auswahl der Testbereiche und -szenarien.
* Förderung des aktiven Informationsaustauschs und Engagements in vertrauenswürdigen Gemeinschaften und Netzwerken für Bedrohungsinformationen und Schwachstellen zur Stärkung der Resilienz.
* Unterstützung bei der Durchführung regelmäßiger, unabhängiger Tests der Schutzmaßnahmen durch Bereitstellung von Risikoeinschätzungen und Überprüfung der Testkonzepte.
* Mitwirkung bei der Sicherstellung der Vertraulichkeit und ordnungsgemäßen Handhabung der Ergebnisse von Tests der digitalen operationalen Resilienz, um die Realitätsnähe und Sicherheit der Tests zu gewährleisten.

*Quelle(n): VO (EU) 2022/2554, Art. 13(1); VO (EU) 2022/2554, Art. 13(3); VO (EU) 2022/2554, Art. 13(4); VO (EU) 2022/2554, Art. 13(7); VO (EU) 2022/2554, Art. 24; VO (EU) 2022/2554, Art. 25; VO (EU) 2022/2554, Art. 26(1); VO (EU) 2022/2554, Art. 26(2); VO (EU) 2022/2554, Art. 26(3); VO (EU) 2022/2554, Art. 26(5); VO (EU) 2022/2554, Art. 26(6); VO (EU) 2022/2554, Art. 26(8); VO (EU) 2022/2554, Art. 27(1); VO (EU) 2022/2554, Art. 27(3)*

*Hinweis: Die Auswahlkriterien und die Verpflichtung zu Threat-Led Penetration Tests (TLPT) nach Art. 26 VO (EU) 2022/2554 werden für eine kleine Bank in der Regel nicht ohne explizite Anforderung der Aufsichtsbehörde relevant. Die Mitwirkung bezieht sich dann primär auf andere Formen der erweiterten Tests gemäß Art. 25.*

# Inkrafttreten

Diese Arbeitsanweisung tritt am TT.MM.JJJJ in Kraft.