					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P40					Dokumenttitel: **Richtlinie zu Sicherheitstests und Red-Team-Übungen**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

Ausgerichtet an Standards und Vorschriften

Standard/Verordnung	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev. 5	CA-2, CA-7, CA-8, RA-5	
EU-DSGVO	Art. 32(1)(d)	
EU-NIS2	Art. 21(2)(f)	
EU-DORA	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Zweck

1 Es wird ein strukturiertes Programm für regelmäßige Sicherheitstests der Netzwerke, Systeme und Anwendungen der Organisation festgelegt, einschließlich Schwachstellenanalysen, Penetrationstests und Red-Team-Übungen, um die Anforderungen aus Artikel 21 Absatz 2 Buchstabe f der NIS2-Richtlinie zur Bewertung der Wirksamkeit von Cybersicherheitsmaßnahmen zu erfüllen.

1.1 Es ist sicherzustellen, dass Schwachstellen in technischen und organisatorischen Maßnahmen durch kontrollierte Tests proaktiv identifiziert und behoben werden, um das Risikoprofil der Informationssicherheit der Organisation kontinuierlich zu verbessern.

2. Geltungsbereich

2 Diese Richtlinie gilt für alle kritischen Informationssysteme, Anwendungen und unterstützenden Infrastrukturen, die sich im Eigentum der Organisation befinden oder von ihr betrieben werden. Sie umfasst zudem physische Sicherheitstests von Standorten, soweit diese für die Cybersicherheit relevant sind, beispielsweise Social-Engineering-Tests oder physische Penetrationstests, sofern sie in den Geltungsbereich von Red-Team-Übungen fallen.

2.1 Diese Richtlinie gilt für interne Sicherheitsteams, beauftragte externe Dienstleister für Sicherheitstests sowie relevante Systemverantwortliche und Anwendungsverantwortliche. Sämtliche Testaktivitäten müssen autorisiert sein und den hierin festgelegten Verfahren folgen, um unbeabsichtigte Störungen zu vermeiden.

3. Ziele

3 Die Wirksamkeit implementierter Cybersicherheitskontrollen (technisch, operativ und organisatorisch) ist durch regelmäßige Tests und Simulationen zu verifizieren, im Einklang mit den NIS2-Vorgaben zur Messung der Wirksamkeit.

3.1 Es sind Schwachstellen oder Lücken aufzudecken, die durch reguläre Betriebsprozesse möglicherweise nicht erkannt werden, einschließlich Zero-Day-Schwachstellen oder Konfigurationsmängeln, unter realitätsnahen Angriffsszenarien (Red Teaming), bevor Bedrohungsakteure diese ausnutzen.

3.2 Der Geschäftsleitung sind durch die Berichterstattung über Testfeststellungen Nachweise und umsetzbare Empfehlungen bereitzustellen, damit fundierte Entscheidungen zur Risikobehandlung und zur kontinuierlichen Verbesserung des Sicherheitsprogramms getroffen werden können.

4. Rollen und Verantwortlichkeiten

4 Koordinator für Sicherheitstests (STC): Vom CISO benannt; verantwortlich für die Planung und Überwachung aller Sicherheitstestaktivitäten. Stellt sicher, dass Tests einen definierten Geltungsbereich haben, autorisiert sind, Ergebnisse berichtet und Folgemaßnahmen umgesetzt werden.

4.1 Internes Sicherheitsteam (Blue Team): Wirkt bei Tests mit, beispielsweise durch Bereitstellung von Informationen für die Festlegung des Geltungsbereichs oder durch Überwachung von Systemen während der Tests. Bei Red-Team-Übungen reagiert das Blue Team auf simulierte Angriffe; seine Erkennungs- und Reaktionsfähigkeit wird bewertet.

4.2 Red Team / Penetrationstester: Kann ein internes Offensiv-Sicherheitsteam oder externe Berater umfassen. Führt Tests nach vereinbarten Einsatzregeln durch, dokumentiert alle festgestellten Schwachstellen und Angriffspfade und wahrt die Vertraulichkeit.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Überwachung und Audit

9 Der STC führt einen Kalender und ein Protokoll aller durchgeführten Sicherheitstestaktivitäten. Dieses Protokoll hat Datum, Geltungsbereich, durchführende Person bzw. Stelle und eine Zusammenfassung der Ergebnisse zu enthalten. Es wird überprüft, um die Einhaltung des vorgeschriebenen Zeitplans sicherzustellen, beispielsweise dass kein kritisches System länger als einen Jahreszyklus ungetestet bleibt.

9.1 Der Fortschritt bei der Behebung von Testfeststellungen wird monatlich überwacht und berichtet. Offene Feststellungen mit hohem Schweregrad werden in Managementsitzungen überprüft, bis sie abgeschlossen sind.

9.2 Die Funktion Interne Revision und Compliance oder ein unabhängiger Auditor überprüft das Programm für Sicherheitstests jährlich, um zu verifizieren, dass Tests ordnungsgemäß autorisiert, durchgeführt und berichtet wurden, dass kritische Feststellungen behandelt wurden und dass das Programm regulatorische Erwartungen erfüllt. Auditoren können beispielsweise prüfen, ob vor dem Start eines neuen Online-Services wie gefordert ein Penetrationstest durchgeführt wurde. Abweichungen führen zu Korrekturmaßnahmenplänen.

10. Überprüfung und Pflege

10 Diese Richtlinie und der übergreifende Testplan werden mindestens einmal jährlich überprüft. Bei der Überprüfung sind Veränderungen der Bedrohungslage zu berücksichtigen, beispielsweise das Aufkommen neuer Angriffstechniken, die durch die aktuellen Tests möglicherweise nicht abgedeckt sind, und Geltungsbereich oder Frequenz entsprechend anzupassen.

10.1 Nach jedem wesentlichen Cybervorfall oder jeder Sicherheitsverletzung ist diese Richtlinie erneut zu prüfen, um festzustellen, ob zusätzliche oder häufigere Tests das Problem hätten verhindern oder früher erkennen können. Die Richtlinie ist anschließend so zu aktualisieren, dass entsprechende Anpassungen aufgenommen werden, beispielsweise durch Aufnahme eines neuen Szenarios in Red-Team-Übungen auf Grundlage beobachteter Angriffsmuster.

10.2 Aktualisierungen dieser Richtlinie müssen durch den CISO genehmigt und dem Leitungsorgan zur Kenntnis gebracht werden. Sämtliches relevantes Personal ist über Änderungen zu informieren; externe Testpartner sind zu benachrichtigen, sofern Änderungen ihre Beauftragungsbedingungen betreffen.

11. Verwandte Richtlinien und Verknüpfungen

11.1 P06 – Risikomanagement-Richtlinie. Testergebnisse steuern die Risikobewertung und Risikobehandlung.

11.2 P22 – Richtlinie zur Protokollierung und Überwachung. Validiert die Erkennungsabdeckung während Übungen.

11.3 P24 – Richtlinie für sichere Softwareentwicklung. Integriert Testfeststellungen in Kontrollen des Software Development Life Cycle (SDLC).

11.4 P25 – Richtlinie zu Anforderungen an die Anwendungssicherheit. Stellt sicher, dass Anforderungen Erkenntnisse aus Tests widerspiegeln.

11.5 P30 – Incident-Response-Richtlinie. Red-Team-Szenarien verfeinern Playbooks und Reaktionsmaßnahmen.

11.6 P31 – Richtlinie zur Beweissicherung und Forensik. Sammelt Artefakte während Tests auf sichere Weise.

11.7 P32 – Richtlinie zur Aufrechterhaltung des Geschäftsbetriebs und Disaster Recovery. Übungen verifizieren die Resilienz unter Angriffen.

11.8 P33 – Richtlinie zur Audit- und Compliance-Überwachung. Unabhängige Überwachung der Wirksamkeit des Programms für Sicherheitstests.

12. Referenzen

12.1 NIS2-Richtlinie (EU 2022/2555), Artikel 21 Absatz 2 Buchstabe f (Richtlinien und Verfahren zur Bewertung der Wirksamkeit von Maßnahmen zum Management von Cybersicherheitsrisiken)

12.2 Durchführungsverordnung (EU) 2024/2690 der Kommission, Anhang Abschnitt 7 (Anforderungen an die Überwachung, Prüfung und Bewertung der Wirksamkeit von Cybersicherheitsmaßnahmen)

12.3 Technische Leitlinien der ENISA (2025) – Anhang zu Sicherheitstests und Audit (Leitlinien zur Durchführung von Cybersicherheitsübungen und technischen Tests)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:

12.5 Bewährte Branchenpraktiken: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (Rahmenwerke für Red Teaming im Finanzsektor als Referenz)