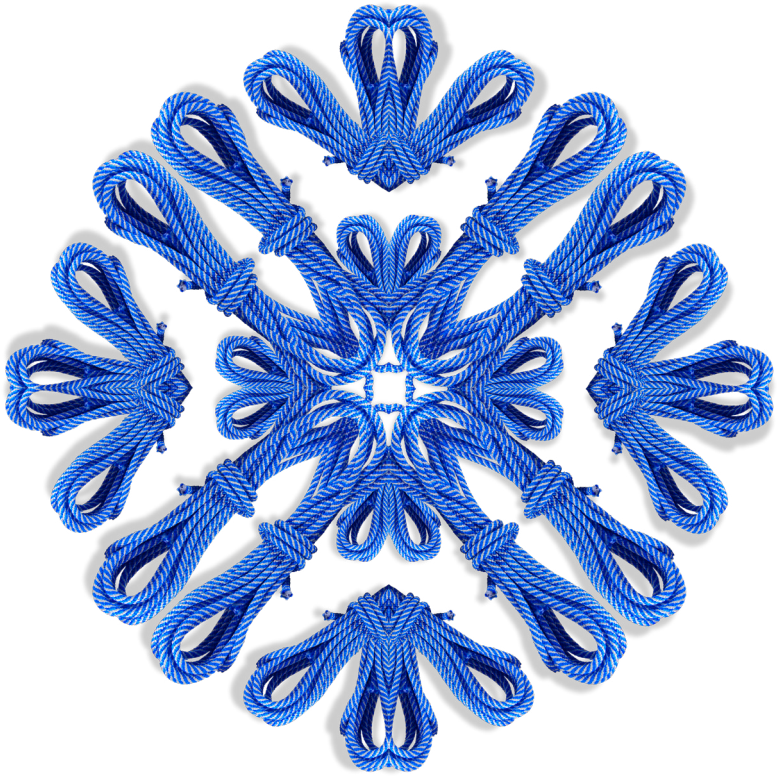
Deloitte.



IKT-Sicherheit

Die Mindeststandards der Finanzmarktaufsicht

Die zunehmende Digitalisierung birgt neben zahlreichen Vorteilen auch neue Risiken und Gefahren für Unternehmen. Immer häufigere und folgenschwerere Cyber-Angriffe machen deutlich, wie verwundbar IT-Systeme sind. Die Leitlinien der Europäischen Bankenaufsichtsbehörde (EBA) konkretisieren grundlegende Anforderungen an IKT-Systeme von Kredit-, Zahlungs- und E-Geldinstituten sowie Wertpapierfirmen.

Die Europäische Bankenaufsicht (EBA) bietet mit den im November 2019 veröffentlichten Leitlinien eine Orientierungshilfe zu Ausgestaltungen, Anforderungen und Vorkehrungen hin sichtlich IKT-Sicherheit und adressiert dabei die aus den Sorgfaltspflichten im § 39 Abs. 2b Z 5 und Abs. 4 BWG sowie aus der Risikomanagementverordnung von Kreditinstituten (insb. § 11 KI-RMV) ableitbaren Anforderungen. Hierdurch ergibt sich auch für den österreichischen Markt eine zentrale Informationsquelle deren Ziel es ist, die Compliance mit nationalen und internationalen Anforderungen an die IT für Kreditinstitute nach § 1 Abs. 1 BWG sowie Zahlungs-, E-Geld, Wertpapierfirmen und ausgewählte Sonderkreditinstitute zu gewährleisten.

Anforderungen

Festgestellte Mängel in der IKT-Sicherheit können sich bei Kreditinstituten auf den SREP-Score auswirken. Um dem vorzubeugen und in Hinblick auf das EBA/GL/2019/04 ergeben sich folgende Anforderungen:

IKT-Strategie, Governance & Risikomanagement

- Einrichtung detaillierter Prozess- und Managementstrukturen der IKT-Landschaft
- Festlegung der strategischen Entwicklung, des IKT-Aufbaus und der IKT-Ablauforganisation inkl. der IKT-Zielarchitektur
- Durchführung von Risikoanalysen und -bewertungen (nach jeder Änderung der Rahmenbedingungen)

Access, Vulnerability & Change Management

- Erstellung einer zentralen Informationssicherheitsrichtlinie sowie genauer themenspezifischer Richtlinien
- Implementierung eines zyklischen Prozesses zur Identifikation und Beseitigung von Schwachstellen
- Festlegung und Dokumentation von regelmäßigen Penetrationstests & Virenscans

Datenintegrität

- Entwurf eines schriftlichen Rahmenwerkes für die Minderung des Datenintegritätsrisikos gemäß BCBS 239 und vergleichbaren Standards und Rahmenwerken

BCM und DRM

- Erstellung eines Rahmenwerkes zur Identifikation, Messung und Begrenzung des Verfügbarkeits- und Kontinuitätsrisikos
- Implementierung von Strategien und Maßnahmen zur Notfallvorsorge, -bewältigung und -nachsorge

Auslagerungsvereinbarungen

- Festlegung von Kriterien, was eine wesentliche IKT-Auslagerung iSd § 25 Abs 2 BWG darstellt
- Berücksichtigung der Anforderungen an Auslagerungsvereinbarungen (EBA/GL/2019/02)

Deloitte Services

- **IKT-Quickscan** zur Durchführung einer Reifegradmessung auf Basis der Schwerpunkte des FMA-Leitfadens
- **Umsetzungsunterstützung und/oder Review von Dokumentationen** z.B. zur IKT-Strategie, zu IKT-Governance-Strukturen oder auch institutsspezifischen IKT-Standards
- **Schulungen und Trainings** zu ausgewählten Themen des IKT-Leitfadens
- **IKT-Gap Analyse** anhand des Scoring-Systems der EBA-GL/2017/05 zum IKT-Risiko unter Berücksichtigung des FMA-Leitfadens, relevanter internationaler Standards sowie verfügbarer Benchmarkings zu vergleichbaren Instituten
- **Security Assessments,** z.B. Penetration Tests, Red Teaming, Vulnerability Scans, Security Operation Centers
- **Optimierung des IKT-Risiko-Scorings** durch Aufarbeitung aufgezeigter Verbesserungspotenziale aus einer IKT-Gap Analyse
- **Vorbereitung auf mögliche Prüfungen** durch die Aufsichtsbehörde und nachfolgende Unterstützung bei der Abarbeitung von aufgezeigten Feststellungen

Ihre Ansprechpersonen

Mag. Alexander Ruzicka
Partner
+43 1 537 00-7950
aruzicka@deloitte.at

Mag. Thomas John
Senior Manager
+43 1 537 00-3723
tjohn@deloitte.at

www.deloitte.at/risk