DORA gemeinsam meistern IKT-Risikokontrolle und Inf

Noch drei Monate – dann sind die DORA-Vorgaben in den Banken umzusetzen. Dazu gehört auch, dass eine IKT-Risikokontrollfunktion einzurichten ist (Art. 6 Abs. 4 DORA). Wie ist diese Funktion praktikabel auszugestalten und wie ist sie mit dem Informationssicherheitsbeauftragten in Einklang zu bringen?

Der bisherige regulative Rahmen

Die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) fordert in den Ziffern 4.4 BAIT ff. die Einrichtung einer unabhängigen Stelle für die Informationssicherheit (ISB).

Die wichtigste Anforderung der BaFin an den Informationssicherheitsbeauftragten ist die Mitwirkung bei der Entwicklung und die Überwachung der Informationssicherheitsstrategie des Unternehmens. Er hat darauf zu achten, dass die geltenden Sicherheitsvorgaben umgesetzt werden. Um nicht in Interessenkonflikte zu geraten, muss der ISB unabhängig agieren können (BAIT Tz. 4.5).
Es ist sicherzustellen, dass er über die notwendige fachliche Kompetenz und Ressourcen verfügt (BAIT Tz. 4.5), die erforderlich für die Bewertung des aktuellen Zustandes der Informationssicherheit sind und ihm erlauben, Maßnahmen zu beschreiben oder zu ergreifen, um die Sicherheitslage zu verbessern. Er berichtet direkt an die Geschäftsführung oder den Vorstand (BAIT Tz. 4.10).

Der ISB berät darüber hinaus die Unternehmensführung in Fragen der Informationssicherheit und informiert sie regelmäßig über den aktuellen Sicherheitsstatus (BAIT Tz. 4.4). Wie die Prüfungspraxis gezeigt hat, legt die BaFin großen Wert darauf, dass der ISB über aktuelle Entwicklungen im Bereich Informationssicherheit informiert ist, denn nur so kann sichergestellt werden, dass Sicherheitsvorfälle schnell erkannt, gemeldet und bearbeitet werden. Zudem sind regelmäßige Risikoanalysen und Schwachstellenprüfungen durch den ISB durchzuführen, um potenzielle Sicherheitsrisiken frühzeitig zu identifizieren und zu beheben.

Schlussendlich darf der ISB zur Sicherung seiner Unabhängigkeit und zur effektiven Wahrnehmung seiner Aufgaben weder in der ersten, noch in der dritten Verteidigungslinie (i.S.d. Modells der „drei Verteidigungslinien“) angesiedelt werden. Er ist ganz klassisch der zweiten Verteidigungslinie zuzuordnen, die neben der kontrollierenden auch eine beratende und schulende Aufgabe innehat.

Der zukünftige regulative Rahmen

DORA (Digital Operational Resilience Act) fordert in Art. 4 Abs. 6 DORA die Einrichtung einer IKT-Risikokontrollfunktion und lässt dabei die Funktion des Informationssicherheitsbeauftragten zunächst unerwähnt. Was heißt das konkret für den ISB und wie muss die IKT-Risikokontrollfunktion ausgestaltet werden.

Aufgaben des Informationssicherheitsbeauftragten
Um es deutlich herauszustellen: Die BaFin hält am ISB fest, obwohl sie die BAIT nach eigener Angabe ersatzlos aufgeben wird (vgl. https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_0708_Interview_Kosche_Steinbrecher.html;jsessionid=31C8B0960EAADB8EE49F593980254EE1.internet981?nn=19669324, abgerufen am 26.09.2024).

– Beauftragter
formationssicherheit

KI-gestützter VertragsCheck auf DORA-Konformität

Die „größte Herausforderung" in diesem Jahr ist DORA und dort die „Überprüfung bestehender Dienstleisterverträge", so das Ergebnis der aktuellen Bankenumfrage 2024 des Genoverbandes e.V. Das deckt sich mit unserer Einschätzung: Die manuelle Prüfung der Verträge ist enorm zeit- und arbeitsaufwendig.

Wir haben deshalb eine KI-gestützte Vollständigkeitsprüfung entsprechend den DORA-Klauseln entwickelt. Das Vertragswerk mit IKT-Drittparteien wird systematisch und nachvollziehbar auf DORA-Konformität untersucht, fehlende Passagen werden erkannt und entsprechende Formulierungsvorschläge aus den BVR-Musterklauseln ausgegeben.

Die Vorteile liegen auf der Hand: Die Bank profitiert

- von einer deutlichen Steigerung der operativen Effizienz;
- von einer sicheren Lösung: Die Vertragsprüfung erfolgt auf Systemen der DZ CompliancePartner GmbH. Es bedarf somit keiner aufwendigen Bewertung eines externen Cloud-Dienstleisters;
- von einer klaren Verbundorientierung: Analysen und Ausgaben basieren einerseits auf Verbundempfehlungen, andererseits auf unserer Expertise aus mehr als 100 Mandaten in der Informationssicherheit.

Das Tool ist bereits im Rahmen unserer DORA-Umsetzungsbegleitung und -beratung im Einsatz. Zukünftig wird es als eine integrale Standardleistung der Auslagerung „Beauftragter IKT-Risikokontrolle und Informationssicherheit" (IKT-Risikokontrollfunktion) angeboten.

Rechtlicher Hinweis: Die Dienstleistung umfasst den Abgleich der relevanten Vertragsklauseln unter Einsatz von KI. Sie stellt keine rechtliche Beratung, Bewertung oder Einschätzung der DORA-Konformität gemäß § 2 des Rechtsdienstleistungsgesetzes (RDG) dar. Die Interpretation der Ergebnisse, rechtliche Bewertungen und Anpassungen von Verträgen liegen in der Verantwortung des Kunden.

DORA fordert ausdrücklich (Art. 5 Abs. 2 lit. c DORA), dass Finanz-institute klare Verantwortlichkeiten für alle IKT-bezogenen Funktionen festlegen. Zwar ändert sich mit DORA der Blickwinkel, die Verordnung folgt einer strikten Risikoperspektive (im Gegensatz zu den BAIT, die eine Sicherheitsperspektive eingenommen hatten). Aber DORA betrachtet die gleichen Inhalte wie die BAIT. Tatsächlich betont sie sogar die Anforderungen an die Informationssicherheit als „den zentralen Baustein der Operativen Resilienz", um das Schutzziel eines verbesserten IKT-Risikomanagements zu erreichen. Insoweit ist nachvollziehbar, warum die BaFin und auch der BVR die in DORA statuierte „IKT-Risikokontrollfunktion" **als ergänzende Aufgabenstellung des bisherigen ISB formulieren.**

Die Beibehaltung des ISB lässt sich darüber hinaus aus der ISO-Norm 27001 herleiten: Die ISO/IEC 27001 verlangt, dass ein Unternehmen eine klar definierte Verantwortung für das Management der Informationssicherheit hat. Das bedeutet, dass bestimmte Aufgaben und Zuständigkeiten für die Informationssicherheit formal festgelegt werden müssen. Dazu gehört die Einrichtung eines Informationssicherheitsmanagementsystems (ISMS). In Klausel 5.3 der ISO 27001 wird zudem festgelegt, dass Rollen und Verantwortlichkeiten für die Informationssicherheit klar benannt werden müssen. Damit ist

nichts anderes als eine ISB-Funktion gemeint.

Des Weiteren sind die vierteljährlichen Berichtspflichten zur Informationssicherheit (MaRisk AT 4.3.2 Tz. 3) weiterhin und somit auch nach dem 17. Januar 2025 vorzunehmen. Die BaFin hat angekündigt, zur Funktion des ISB nochmal gesondert Stellung zu nehmen.

Zusammenfassend werden mit Inkrafttreten von DORA die Anforderungen an den ISB eher erweitert. Der ISB wird im Zusammenspiel mit der IKT-Risikokontrollfunktion eine wichtige Rolle spielen, die EU-weiten Anforderungen aus DORA umzusetzen und damit schlussendlich die operative Resilienz der Bank sicherzustellen.

Aufgaben der IKT-Risikokontrollfunktion

Die IKT-Risikokontrollfunktion (Art. 6 Abs. 4 DORA) ist eine zentrale Komponente von DORA. Sie bezieht sich auf die organisatorischen und prozessualen Maßnahmen, die ein Finanzinstitut ergreifen muss, um die Risiken im Zusammenhang mit der IT-Infrastruktur, den IT-Prozessen und der Cybersicherheit zu kontrollieren und zu überwachen.

Gemäß Art. 6 Abs. 4 S. 2 DORA ist die IKT-Risikokontrollfunktion – genau wie der ISB – in der „zweiten Verteidigungslinie“ anzusiedeln und mit entsprechenden Mitteln und Befugnissen auszustatten.

Versteht man diese Funktion also sachgerecht als Weiterentwicklung der bisherigen ISB-Funktion nach BAIT (s.o.), so bleiben nur ergänzende Aufgaben. Zentrale Punkte sind hierbei

- die Bewertung der Risikoposition gegen Cyberrisiken und
- die Bewertung der Resilienz bzw. Widerstandsfähigkeit der IKT-Risiken sowie
- die entsprechende Berichterstattung (Art. 6 Abs. 5 DORA).

Es sind ergänzende „High-Level“ Risikokontrollen einzuführen und zu berichten, um hieraus Maßnahmen ableiten zu können (inkl. Umsetzungsstand der Maßnahmen). Die Funktion bildet damit die Überwachung des IKT-Risikomanagementrahmens mit ab.

Fazit

Das bewährte System der ISB-Funktion kann und sollte beibehalten und durch die Aufgaben der IKT-Risikokontrollfunktion ergänzt werden.
Dies spart ein Neuaufsetzen an sich bewährter Prozesse und ermöglicht eine nahtlose Zusammenführung der Aufgaben – ohne System- und Prozessbrüche. Die neue Funktion ist am besten als „Beauftragte(r) IKT-Risikokontrolle und Informationssicherheit“ zu verstehen. Die Stellenbeschreibung des bisherigen ISB ist entsprechend anzupassen.
Die DZ CompliancePartner GmbH wird ab dem 17. Januar 2025 den Beauftragten IKT-Risikokontrolle und Informationssicherheit (IKT-Risikokontrollfunktion) in der Vollauslagerung anbieten. ▬

Marc-Timo Brandenburger
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: marc-timo.brandenburger@dz-cp.de

Benjamin Wellnitz
Bereichsleiter Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de