GEGENÜBERSTELLUNG VON ANFORDERUNGEN AN DIE DOR- & DIE IT-STRATEGIE

Anforderungen an die IT-Strategie (BAIT+MaRisk)

Anforderungen	Referenz BAIT/ MaRisk
Die IT-Strategie muss zusätzlich zur Informationssicherheit auch allgemeine strategische IT-Ziele sowie Maßnahmen zur Zielerreichung enthalten.	BAIT 1.1.
Die IT-Strategie muss Aussagen zur strategischen Entwicklung der IT-Aufbau- und IT-Ablauforganisation sowie Informationen zu IT-Dienstleistungen und Abhängigkeiten von Dritten beinhalten	BAIT 1.2.a
Die IT-Strategie muss Aussagen zu IT- und Informationssicherheitsstandards enthalten	BAIT 1.2.b
Die IT-Strategie muss Aussagen zur Zuständigkeit und Einbindung des ISB beinhalten	BAIT 1.2.c
Die IT-Strategie muss Aussagen zum IT-Notfallmanagement beinhalten	BAIT 1.2.e
Die IT-Strategie muss Aussagen zum Thema IDV-Management beinhalten	BAIT 1.2.f
Die IT-Strategie muss einem Strategieprozess unterliegen, der die Phasen Planung, Umsetzung, Beurteilung und Anpassung beinhaltet und Ursachenanalysen für Abweichungen vorsieht	MaRisk AT 4.2, Ziffer 5
Anpassungen an der IT-Strategie sind mit dem Aufsichtsrat zu erörtern	MaRisk AT 4.2, Ziffer 6
Die IT-Strategie ist innerhalb des Instituts in geeigneter Weise zu kommunizieren.	MaRisk AT 4.2, Ziffer 7

Vergleichbare Anforderungen an IT- & DOR-Strategie

Referenz BAIT/ MaRisk	Anforderungen	Referemz DORA-VO
BAIT 1.2.	Beide Strategien müssen aufzeigen, wodurch/ wie sie die Geschäftsstrategie und Geschäftsziele unterstützen	Art. 6, Abs. 8(a) DORA
BAIT, 1.1., sowie MaRisk AT 4.2, Ziffer 2	Sowohl IT-Strategie als auch DOR-Strategie müssen Angaben zur Risikotoleranzschwelle für (gemäß DORA-VO) bzw. zum Risikoappetit (gemäß BAIT/MaRisk) enthalten.	Art. 6, Abs. 8(b) DORA
BAIT 1.2. (c)	Beide Strategien müssen die Ziele der Informationssicherheit beinhalten ,	Art. 6, Abs. 8(c) DORA
BAIT 1.2. (d)	Sowohl IT-Strategie als auch DOR-Strategie müssen Informationen zur geplanten strategischen Entwicklung der IT-Architektur enthalten	Art. 6, Abs. 8(d) DORA
BAIT 1.2/ MaRisk AT 4.2, Ziffer 4	Für die Festlegung und Genehmigung der IT-Strategie und der DOR-Strategie ist das Leitungsorgan verantwortlich	Art. 5, Abs. 2(d) DORA
BAIT, 1.1., MaRisk AT 4.2, Ziffer 5	Für beide Strategien muss die Wirksamkeit der Umsetzung überwacht werden	Art. 13, Abs. 4 DORA
BAIT 1.2/ MaRisk AT 4.2, Ziffer 4	Bei beiden Strategien muss das Leitungsorgan eine aktive Rolle einnehmen und für die Umsetzung Sorge tragen	ErwGr 45 DORA
BAIT 9.3, MaRisk AT 4.2, Ziffer 1, Bemerkungen	Für beide Strategien muss sichergestellt werden, dass der Bezug von IKT-Dienstleistungen im Einklang mit IT- bzw. DOR-Strategie steht.	Art. 6, Abs. 9 DORA Art. 29, Abs. 1 DORA

Anforderungen an die DOR-Strategie (DORA-VO)

Anforderungen	Referemz DORA-VO
Die DOR-Strategie muss Angaben zur Auswirkungsstoleranz mit Blick auf IKT-Störungen enthalten.	Art. 6, Abs. 8(b) DORA
Die DOR-Strategie muss Angaben Security-KPI und Risk Metrics enthalten.	Art. 6, Abs. 8(c) DORA
Die DOR-Strategie soll einen Überblick über die (bestehende) IT-Architektur enthalten.	Art. 6, Abs. 8(d) DORA
Die DOR-Strategie muss Informationen zu den im Einsatz befindlichen Detection- und Prevention Mechanismen und Tools zur Erkennung und zum Schutz von/vor IKT-Incidents beinhalten.	Art. 6, Abs. 8(e) DORA
Die DOR-Strategie muss Ausführungen zum aktuellen Stand der digitalen operationalen Resilienz anhand der Anzahl gemeldeter schwerwiegender IKT- Vorfälle und der Wirksamkeit von Präventivmaßnahmen enthalten.	Art. 6, Abs. 8(f) DORA
Die DOR-Strategie muss Ausführungen zu Tests der digitalen operationalen Resilienz beinhalten	Art. 6, Abs. 8(g) DORA
Die DOR-Strategie muss Ausführungen zur Kommunikationsstrategie von IKT-Incidents beinhalten.	Art. 6, Abs. 8(h) DORA
Anpassungen an den Policies & Procedures müssen hinsichtlich der Auswirkungen auf die DOR-Strategie analysiert werden	Art. 27, Abs. 2(f) RTS ICT risk framework
Policies und Procedures müssen an der DOR-Strategie ausgerichtet sein und sollen einen Verweis beinhalten, der eine Überprüfung der Dokumente vorsieht, sobald Änderungen an der DOR-Strategie vorgenommen werden	Art. 2, Abs. 2(a) RTS ICT risk framework, Art. 3, Abs. 1(f) RTS ICT risk framework, ErwGr 3 RTS ICT risk framework

© Copyright 2024 | Dr. Marlen Hofmann | Alle Inhalte, insbesondere Texte, Fotografien und Grafiken sind urheberrechtlich geschützt. Alle Rechte, einschließlich der Vervielfältigung, Veröffentlichung, Bearbeitung und Übersetzung, bleiben vorbehalten.