ANFORDERUNGEN AN DIE DOR-STRATEGIE

Dokument	Strategie für die digitale operationale Resilienz (DOR-Strategie)
Typ	

Anforderung	Inhaltliche Anforderungen		Formale & prozessuale Anforderungen	
	Die DOR-Strategie zeigt auf, wodurch/ wie die Geschäftsstrategie und Geschäftsziele unterstützt werden	Art. 6, Abs. 8(a) DORA	Die DOR-Strategie muss als Basis für die Ausgestaltung des IKT-Risikomanagementrahmens herangezogen werden	Art. 6, Abs. 8 DORA
	Die DOR-Strategie beinhaltet Angaben zur Risikotoleranzschwelle für IKT-Risiken sowie die Auswirkungstoleranz mit Blick auf IKT-Störungen	Art. 6, Abs. 8(b) DORA	Das Leitungsorgan trägt die Gesamtverantwortung für die Festlegung und Genehmigung der DOR-Strategie	Art. 5, Abs. 2(d) DORA
	Die DOR-Strategie beinhaltet Ziele der Informationssicherheit, Security-KPI und Risk Metrics (z.B Anzahl von IKT-Incidents, Anzahl und Schweregrad von IKT-Risiken, durchschnittlicher Zeitbedarf zur Beseitigung von Schwachstellen, etc.)	Art. 6, Abs. 8(c) DORA	Die Wirksamkeit der Umsetzung der DOR-Strategie muss überwacht werden	Art. 13, Abs. 4 DORA
	Die DOR-Strategie beinhaltet einen Überblick über die IT-Architektur sowie geplante Änderungen, um die Geschäftsziele zu erreichen	Art. 6, Abs. 8(d) DORA	Das Leitungsorgan nimmt eine aktive Rolle bei der Erstellung und dem Management der DOR-Strategie ein	ErwGr 45 DORA
	Die DOR-Strategie beinhaltet Informationen zu Mechanismen und Tools, (1) die zur Erkennung von IKT-Incidents eingesetzt werden (Detection Tools), (2) die zum Schutz vor IKT-Incidents eingesetzt werden (Prevention Tools) und die potentiellen Folgen verhindern (Response/ Contain Tools)	Art. 6, Abs. 8(e) DORA	Anpassungen am ICT risk management framework müssen hinsichtlich der Auswirkungen auf die DOR-Strategie analysiert werden	Art. 27, Abs. 2(f) RTS ICT risk framework
	Die DOR-Strategie beinhaltet Ausführungen zum aktuellen Stand der digitalen operationalen Resilienz anhand der Anzahl gemeldeter schwerwiegender IKT- Vorfälle und der Wirksamkeit von Präventivmaßnahmen	Art. 6, Abs. 8(f) DORA	Sofern das Finanzunternehmen eine Strategie zur Nutzung mehrerer IKT-Anbieter auf Gruppen- oder Unternehmensebene festlegt, ist diese mit der DOR-Strategie zu alignen	Art. 6, Abs. 9 DORA
	Die DOR-Strategie beinhaltet Ausführungen zu Tests der digitalen operationalen Resilienz	Art. 6, Abs. 8(g) DORA	Vor Abschluss von IKT-Verträgen, ist die Konformität zur DOR-Strategie zu prüfen	Art. 29, Abs. 1 DORA
	Die DOR-Strategie beinhaltet Ausführungen zur Kommunikationsstrategie von IKT-Incidents	Art. 6, Abs. 8(h) DORA	Policies und Procedures, die von DORA gefordert sind, müssen an der DOR-Strategie ausgerichtet werden und einen inhaltlichen Verweis auf einen Prozess beinhalten, der sicherstellt, dass Änderungen an der DOR-Strategie in den Policies und Procedures berücksichtigt 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