Patrick Buchmüller | Gerhard Hellstern

IT-Risiken in Banken

Aufsichtliches Rahmenwerk für die Digitale Transformation

SCHÄFFER
POESCHEL

Gerhard Hellstern/Patrik Buchmüller

IT-Risiken in Banken

Aufsichtliches Rahmenwerk für die Digitale Transformation

1. Auflage

Schäffer-Poeschel Verlag Stuttgart

Bibliografische Information der Deutschen Nationalbibliothek

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.dnb.de abrufbar.

Print: ISBN 978-3-7910-4536-8 Bestell-Nr. 12007-0001
ePub: ISBN 978-3-7910-4537-5 Bestell-Nr. 12007-0100
ePDF: ISBN 978-3-7910-4538-2 Bestell-Nr. 12007-0150

Gerhard Hellstern/Patrik Buchmüller
IT-Risiken in Banken
1. Auflage, August 2019

www.schaeffer-poeschel.de
service@schaeffer-poeschel.de

Produktmanagement: Frank Katzenmayer

Inhaltsverzeichnis

1 Vorwort und Einführung ... 7

2 Rechtsgrundlagen für Vorgaben zur Bank-IT ... 13
2.1 Rechtsinstrumente und Akteure im Überblick ... 13
2.2 Die BAIT im Kontext des deutschen und EU-Bankenaufsichtsrechts ... 15
2.2.1 KWG, CRD und EBA ... 15
2.2.2 Rechtliche Einordnung der BAIT ... 18
2.2.3 Fortentwicklung der BAIT ... 21
2.3 Regulierung und Überwachung von EBA und EZB ... 23
2.3.1 Leitlinien der EBA mit Bezug zu IT-Risiken ... 23
2.3.2 EZB-Bankenaufsicht und EZB in Zentralbankfunktion ... 31
2.3.3 ESA-Advice vom April 2019 ... 34
2.4 Tätigkeiten des Baseler Ausschusses und weiterer internationaler Gremien ... 37
2.4.1 Arbeiten des Baseler Ausschusses zur IT-Regulierung ... 37
2.4.2 Tätigkeit des Financial Stability Board zu Cyber Security ... 41
2.4.3 Vorgaben zur IT-Sicherheit auf Ebene der G7 ... 43
2.5 Die Tätigkeit des BSI mit Bezug zur IT-Sicherheit der Banken ... 51
2.5.1 Einführung in die Tätigkeit des BSI ... 51
2.5.2 BSI-Grundschutz ... 53
2.5.3 BSI-Aufgaben im Bereich Kritische Infrastruktur ... 54

3 Bankaufsichtliche Anforderungen an die IT (BAIT) ... 57
3.1 Vorbemerkung der BAIT ... 58
3.2 IT-Strategie ... 62
3.3 IT-Governance ... 64
3.4 Informationsrisikomanagement ... 68
3.5 Informationssicherheitsmanagement ... 73
3.6 Benutzerberechtigungsmanagement ... 77
3.7 IT-Projekte, Anwendungsentwicklung (inkl. durch Endbenutzer in den Fachbereichen) ... 80
3.8 IT-Betrieb (inkl. Datensicherung) ... 84
3.9 Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen ... 87
3.10 Kritische Infrastrukturen ... 91
3.11 Beurteilung der BAIT ... 93

4 Orientierungshilfe zu Auslagerungen an Cloud-Anbieter ... 95
4.1 Einführung in das Thema Cloud ... 95

4.2 Struktur des Merkblatts und wichtige Aspekte ... 96
4.3 Analyse und Wesentlichkeitsbewertung ... 97
4.4 Vertragsgestaltung bei (wesentlicher) Auslagerung ... 99
4.5 Beurteilung des Merkblatts ... 103

5 Anstehende Erweiterungen der Vorgaben und angrenzende Regelungen ... 105
5.1 EBA Guidelines on ICT and Security Risk Management ... 105
5.1.1 Überblick über den EBA-Entwurf vom 13.12.2018 ... 105
5.1.2 Neuerungen im Detail ... 108
5.1.3 Vorgaben zu IT-Projekten im Detail ... 110
5.2 Weitere IT-Rechtliche Entwicklungen ... 111
5.2.1 IT Sicherheitsgesetz 2.0 und Anpassung der KRITIS-VO ... 111
5.2.2 Weitere EU-rechtliche Initiativen zur IT-Sicherheit ... 115
5.3 Fintech und Künstliche Intelligenz ... 117

6 Zusammenfassung und Ausblick ... 121

Literatur ... 125
Stichwortverzeichnis ... 131
Autoren ... 137