KSW
KAMMER
DER STEUERBERATER
UND WIRTSCHAFTSPRÜFER

Unser Zeichen 1283/18/RK

Sachbearbeiter Mag. Kovacs

Telefon +43 | 1 | 811 73-235

eMail kovacs@ksw.or.at

Datum 21. März 2018

FINANZMARKTAUFSICHT
Bereich Bankenaufsicht
z.H. Frau Julia Ehgartner, LLB,
Otto-Wagner-Platz 5
1090 Wien
mailto:konsultation.RS.APVO@fma.gv.at

**Stellungnahme zum Entwurf des Leitfadens „IT-Sicherheit in Kreditinstituten“**
(GZ: FMA-SG23 5000/0033-DEZ/2018)

Sehr geehrte Frau Ehgartner,

die Kammer der Steuerberater und Wirtschaftsprüfer dankt für die Einladung zur Abgabe einer Stellungnahme zum Entwurf des Leitfadens „IT-Sicherheit in Kreditinstituten“.

## Stellungnahme

### A. Inhaltliches

### Abschnitt 3.
### IT-Governance

**Zu Abs. 3:**

Die KSW empfiehlt den dritten Absatz, beginnend mit „Die Geschäftsleitung stattet das IT-Risikomanagement….“, wie folgt zu ergänzen:

Die Geschäftsleitung stellt weiterhin sicher, dass ein in Bezug auf Aufbau und Ausführung angemessenes Internes Kontrollsystem (IKS) gemäß § 39 Abs. 2 Z 5 und Abs. 4 BWG in Verbindung mit § 11 KI-RMV eingerichtet und dokumentiert ist.

KSW
KAMMER
DER STEUERBERATER
UND WIRTSCHAFTSPRÜFER

**Zu Abs. 4:**

Wir regen an, den vierten Absatz, beginnend mit „Institute verfügen über Prozesse....", wie folgt zu ergänzen:

Insbesondere ist darauf zu achten, dass diese Themen entsprechend § 42 BWG im Zuge von Prüfungen durch die Interne Revision berücksichtigt werden bzw. durch Einbeziehung externer Experten auf Effektivität zu überprüfen sind.

## Abschnitt 5.1.
## Informationssicherheitsmanagement

**Zu Abs. 2:**

Wir empfehlen, in Absatz 2 beginnend mit „Die Informationssicherheitsrichtlinie ist Ausgangspunkt...." in der Aufzählung der Prozesse und Teilbereiche das Thema „physische Sicherheit/Absicherung der Gebäude und Datacenter" zu ergänzen.

## Abschnitt 6.
## IT-Projekte und Anwendungsentwicklung

**Zu Abs. 4 zweiter Satz:**

Der zweite Satz in Abschnitt 6. Abs. 4 lautet:
„In diesem Zusammenhang werden neben der Produktionsumgebung entsprechende Entwicklungs- und Testumgebungen implementiert."

Im Gegensatz zu den ICT Guidelines (56.c: „test environments that adequately reflect production environments"), die nur von Testumgebungen sprechen, wird im Leitfaden – ungeachtet der Art der Anwendungen – eine 3-System-Landschaft als Norm betrachtet.

Der dem zweiten Satz in Abschnitt 6. Abs. 4 nachfolgende Satz lautet:
„Diese geben die Produktionsumgebung effizient wieder."

Die Bedeutung von „effizient" ist in dem Zusammenhang unklar.

## Abschnitt 8.
## IT-Auslagerungen

Lässt sich aus der Verbindung zu § 25 BWG ableiten, dass die Anforderungen des Leitfadens „IT-Sicherheit in Kreditinstituten" ebenfalls durch den Dienstleister (Service Organisation) gänzlich zu erfüllen sind, sofern es sich um eine Auslagerung wesentlicher bankbetrieblicher Aufgaben handelt?

KSW
KAMMER
DER STEUERBERATER
UND WIRTSCHAFTSPRÜFER

## B. Formales

### Abschnitt 1.
### Rechtsgrundlagen und Grundlegendes

**Zu Seite 5 – CoBIT:**

Die Abkürzung ist in der Überschrift und in den darauffolgenden zwei Sätzen falsch geschrieben – es muss jeweils COBIT lauten.

### Abschnitt 5.2.
### Benutzerberechtigungsmanagement

**Zu Abs. 3 erster Satz:**

Der erste Satz in Abschnitt 5.2. Abs. 3 lautet:

„Das Institut verfügt über ein dokumentiertes Berechtigungskonzept bzw. Benutzerberechtigungsprozesse."

Steht hier das Wort „bzw." in der Bedeutung von „und" oder „oder"?

Wir ersuchen höflich, unsere Vorschläge bzw. Anregungen zu berücksichtigen und verbleiben

mit freundlichen Grüßen

Mag. Gerhard Marterbauer e.h.
(Vorsitzender des Fachsenats für
Unternehmensrecht und Revision)

Dr. Gerald Klement
(Kammerdirektor)

Referenten:
Mag. Christian Grinschgl
Mag. Andrea Stippl