



X-WERT
BankTechnology GmbH



Auslagerung des Beauftragtenwesens

Informationssicherheit



Markus Geiß
Februar 2020



Für das Jahr 2020 hat die BaFin vier Schwerpunktthemen festgelegt, die für alle Geschäftsbereiche große Bedeutung haben:

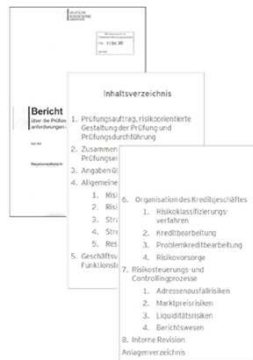
1. Digitalisierung, IT- und Cyberrisiken
2. Integrität des Finanzsystems und Bekämpfung von Finanzkriminalität
3. Nachhaltige Geschäftsmodelle
4. Nachhaltige Finanzwirtschaft, Sustainable Finance

Diese Aufsichtsschwerpunkte leiten sich aus den strategischen Zielen der BaFin ab – und prägen die Aufsichts- und Prüfungsplanung für das Jahr 2020. Zudem bringt die BaFin ihre Positionen im Sinne einer stärkeren aufsichtlichen Konvergenz aktiv in die internationale Gemeinschaft der Aufseher und Regulierer ein. Im Mittelpunkt steht dabei die Zusammenarbeit mit der Europäischen Zentralbank (EZB) und den Europäischen Aufsichtsbehörden (ESAs).

In einer zunehmend digitalen Finanzwelt stellt die **IT- und Cybersicherheit** der beaufsichtigten Unternehmen weiterhin einen Aufsichtsschwerpunkt dar. Dies gilt insbesondere, da der überwiegende Teil der IT-Sicherheitsvorfälle bei Finanzmarktteilnehmern auf hausinterne Schwächen der Unternehmen zurückzuführen ist – und nur zu einem kleineren Teil auf externe Angriffe.

Quelle: https://www.bafin.de/DE/Aufsicht/Aufsichtsschwerpunkte/Aufsichtsschwerpunkte_2020/aufsichtsschwerpunkte2020_node.html

Allgemeine Prüfungsschwerpunkte im IT Umfeld



- ▶ IT-Strategie
- ▶ Informationssicherheit (IT-Sicherheitsbeauftragter)
- ▶ Benutzerberechtigungskonzepte
- ▶ Notfallkonzepte
- ▶ Schutzbedarfsklassen
- ▶ Testkonzepte bei Anwenderentwicklungen
- ▶ Auslagerung und Fremdbezug (Auslagerungsmanagement)



Rechte und Pflichten eines Sonderprüfers



Rechte:

- ▶ Umfassendes Auskunfts- und Unterlagenvorlagerecht
- ▶ Umfassendes Prüfungsrecht
- ▶ Recht zum Betreten und Besichtigen der Geschäftsräume
- ▶ Recht zur Einholung einer Vollständigkeitserklärung
- ▶ Recht zur Durchführung eines Sachverhaltsabgleichs
- ▶ Recht auf Erstattung der Prüfungskosten

Pflichten:

- ▶ Pflicht zur Bestätigung der Auftragsannahme (um Ausschlussgründe zu vermeiden)
- ▶ Anzeigepflicht nach § 29 Abs. 3 KWG (Weitergabe von Informationen an die BaFin)

IT Strategie

- Keine schriftlich festgelegte IT-Strategie
- Fehlende Rollenbeschreibung in der IT-Strategie
- Keine Budgetierung von IT-Aufbau und Organisation

Schutzbedarfs- ermittlung

- Fehlende Schutzbedarfsermittlung für alle relevanten Ziele der Informationssicherheit
- Risikoanalyse und für Risikostreuung unberücksichtigte OpRisks mit schwerwiegenden negativen Auswirkungen (auch Transparenz)

Notfallkonzept

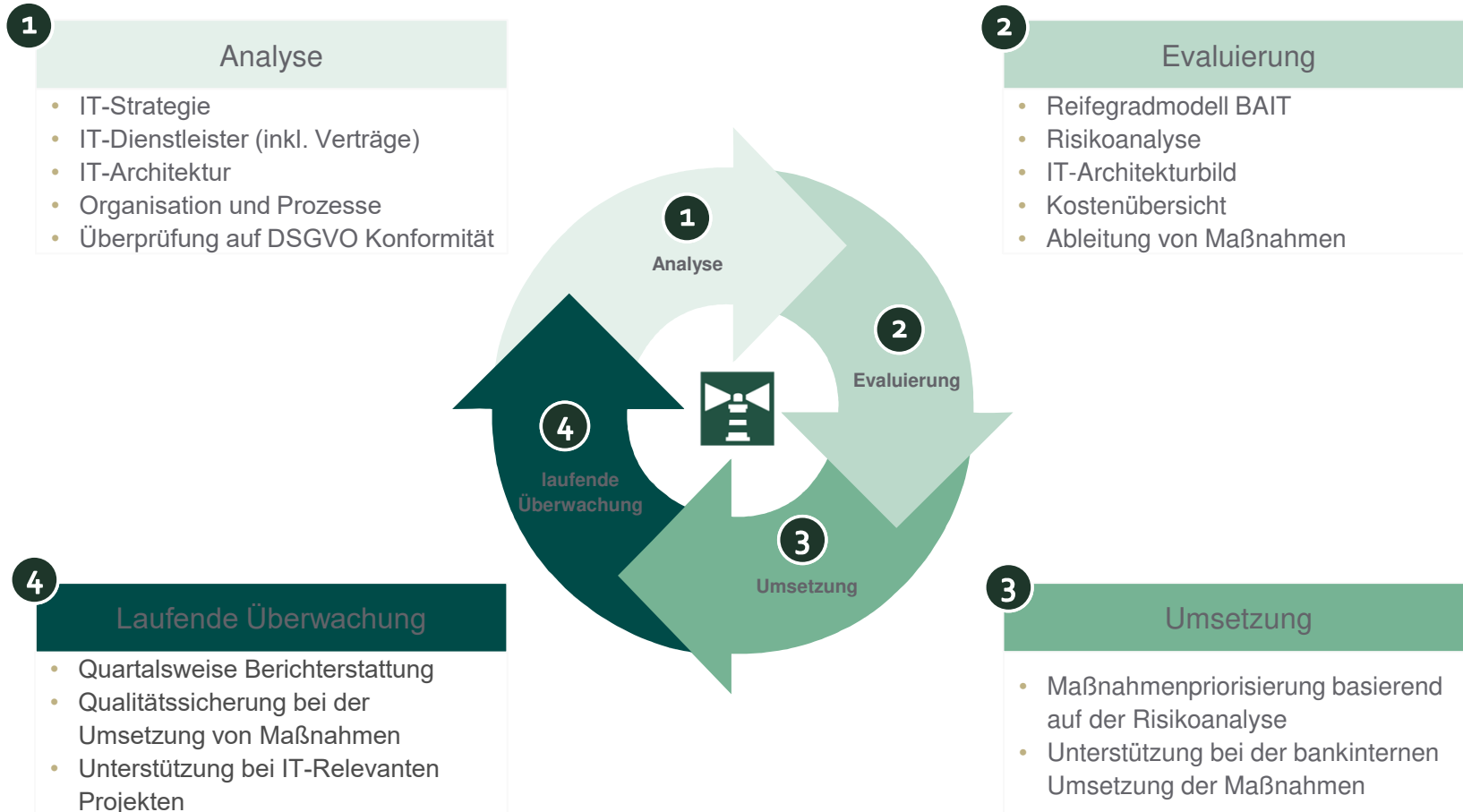
- Kein Notfallkonzept
- Keine festgelegten Verantwortlichkeiten für zentrale Koordination
- Zeitkritische Prozesse und mögliche Bedrohungsszenarien nicht ermittelt
- Keine abteilungsübergreifende abgestimmte Notfallplanung

Benutzer- berechtigung

- Fehlende unabhängige Prüfung auf Notwendigkeit und Zulässigkeit von Benutzerrechten
- Fehlende regelmäßige Überprüfung

Auslagerung

- Keine angemessener Überwachung und Steuerung der Auslagerung
- Keine Einbindung in das IKS, daher schwerwiegende negative Auswirkung auf IT-Sicherheit, BCM und Ermittlung OpRisk



Kontakt

X-Wert BankTechnology GmbH
Behringstraße 28a
22765 Hamburg
Deutschland

Telefon: +49 40 303 77 40 0
Telefax: +49 40 303 77 40 0
E-Mail: info@x-wert.de

Ihr Ansprechpartner:

Dr. Carsten Müller
Geschäftsführender Gesellschafter

Mobil: +49 173 5470157
E-Mail: carsten.mueller@x-wert.de

KWF Business Consultants S.A.
3, Schaffmill
6778 Grevenmacher
Luxemburg

Telefon: +352 26 350 333 1
Telefax: +352 26 350 433
E-Mail: info@kwf.lu

Ihr Ansprechpartner:

Christian Kistler
Managing Director

Mobil: +49 172 6554466
E-Mail: christian.kistler@kwf.lu

KWF Business Consultants GmbH
Bettinastraße 30
60325 Frankfurt am Main
Deutschland

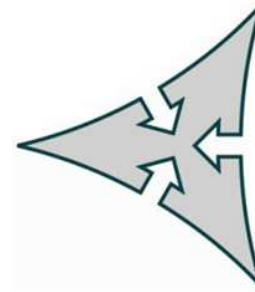
Telefon: +49 69 577 038 20
Telefax: +49 69 577 038 24
E-Mail: info@kwf-consultants.de

© 2020 by KWF Business Consultants, L-Grevenmacher/D-Frankfurt am Main / X-Wert BankTechnology GmbH, Hamburg

Das vorliegende Dokument ist urheberrechtlich geschützt. Kein Teil davon darf ohne schriftliche Einwilligung der KWF Business Consultants oder X-Wert BankTechnology in irgendeiner Form (Fotokopie, Mikrofilm oder ein anderes Verfahren), auch nicht zum Zwecke der Unterrichtsgestaltung, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Zitate und Nachdrucke, auch auszugsweise, sind nur mit ausdrücklicher Genehmigung und Quellenhinweisen gestattet.



X-WERT
BankTechnology GmbH



KWF
Business Consultants



SERVICE

A person in a black tuxedo jacket, white shirt, and white gloves is holding a purple garment. The person is also holding a red-handled cane.

BEST PRACTICE

A compass is shown on a dark, textured rock surface. The compass face is black with white markings and a gold-colored rim.