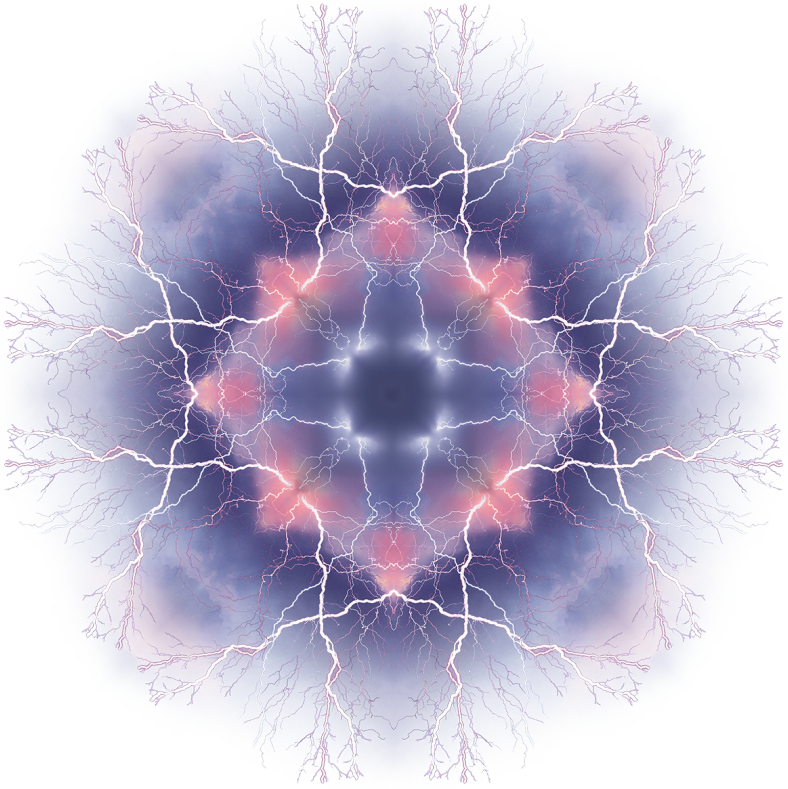
Deloitte.



Business Continuity Management

Alles steht still – nichts funktioniert – was nun?

Hardware- oder Softwareversagen und der gesamte Geschäftsbetrieb kommt zu Erliegen.

Speziell in solch einer Situation, zeigt sich nicht nur die Abhängigkeit von IT-Systemen, sondern auch oftmals die Hilflosigkeit aller Beteiligten bei der Lösung des Problems.

Die IKT-Leitfäden der Finanzmarktaufsicht (FMA) legen erste Anforderungen im Umgang mit solch einem Verfügbarkeits- und Kontinuitätsrisiko sowie ein angemessenes Notfallmanagement fest. Auch in der aktuellen Leitlinie (EBA/GL/2019/04) der Europäischen Bankenaufsichtsbehörde (EBA) werden die Anforderungen eines Business Continuity Managements nicht nur im Detail beschrieben, sondern von Kredit-, Zahlungs- und E-Geldinstituten sowie Wertpapierunternehmen ab 30. Juni 2020 konkret gefordert.

Die Finanzmarktaufsicht bietet mit den in 2018 veröffentlichten Leitfäden erste Orientierungshilfen im Umgang mit bestehenden Verfügbarkeits- und Kontinuitätsrisiken und fordert ein Rahmenwerk bzw. ein adäquates Notfallmanagement um kritische Ressourcen und Prozesse zu schützen bzw. rasch wiederherzustellen. Sie adressiert dabei die aus den Sorgfaltspflichten im § 39 Abs. 2b Z 5 und Abs. 4 BWG sowie aus der Risikomanagementverordnung von Kreditinstituten (insb. § 11 KI-RMV) ableitbare Anforderungen. Neben den IKT-Leitfäden der FMA, wird in der ISO 22301:2019 als auch der am 28.11.2019 veröffentlichten Leitlinie der Europäischen Bankenaufsichtsbehörde (EBA/GL/2019/04) konkret auf die Umsetzung eines Business Continuity Managements eingegangen. Hier sind besonders die Anforderungen der Europäischen Bankenaufsichtsbehörde an ein Business Continuity Management für österreichische Kredit-, Zahlungs- und E-Geldinstitute sowie Wertpapierunternehmen hervorzuheben, da diese mit 30. Juni 2020 verpflichtend einzuhalten sind.

Anforderungen an ein Business Continuity Management in Hinblick auf EBA/GL/2019/04

Business Impact Analysis (BIA)

- Quantitative und/oder qualitative Bewertung der Auswirkungen potentieller Risiken anhand interner und/ oder externer Daten und Szenarioanalysen
- Ausrichtung der IKT-Systeme und -Services anhand der Ergebnisse der BIA (z.B. Redundanz bestimmter kritischer Komponenten)

Business Continuity Planning

- Erarbeitung von Plänen, welche sicherstellen, dass auf potentielle Ausfallszenarien angemessen reagiert werden kann
- Berücksichtigung verschiedener Szenarien, einschließlich extremer, aber plausibler Ereignisse wie z.B. mögliche Auswirkungen eines Cyber-Angriffs

Notfallpläne

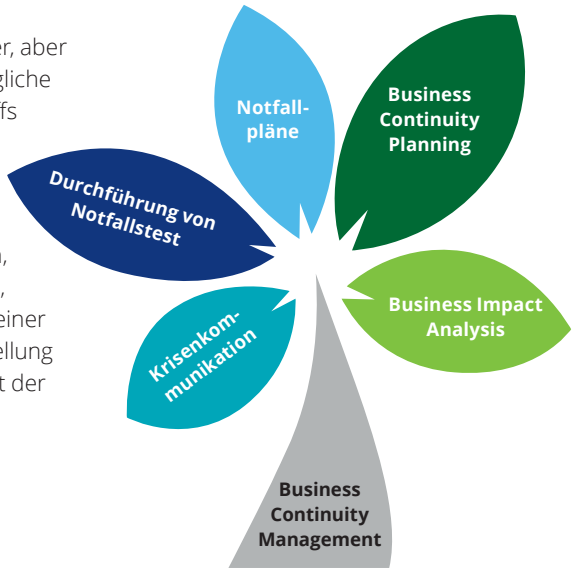
- Erarbeitung angemessener Notfallpläne, welche sicherstellen, dass anhand definierter Kriterien, geeignete Maßnahmen zum Ziel einer schnellstmöglichen Wiederherstellung der Verfügbarkeit und Kontinuität der IKT-Systeme umgesetzt werden

Durchführung von Notfalltests

- Prüfung der Business Continuity Pläne auf Funktionsfähigkeit zur Wiederherstellung kritischer IKT-Systeme
- Aktualisierung bzw. Überarbeitung der Business Continuity Pläne auf Basis der Testergebnisse

Krisenkommunikation

- Sicherstellung einer zeitnahen und angemessenen Kommunikation während einer Störung, eines Notfalls bzw. der Umsetzung der Business Continuity Pläne



Deloitte Services

Definition von BCM-Plänen (intern/ extern)
unter Berücksichtigung verschiedenster Szenarien wie z.B. mögliche Auswirkungen eines Cyber-Angriffs

Definition von Kennzahlen für Auslagerungen (Outsourcing)
z.B. Recovery Time Objective (RTO) und Recovery Point Objective (RPO)

Konsolidierung von BCM-Plänen
zur Sicherstellung und Erarbeitung eines institutsweiten BCM-Plans

Schulungen und Trainings
zu ausgewählten Themen des Business Continuity Managements

Umsetzungsunterstützung und/oder Review von Dokumentationen
zur Business Impact Analyse, dem Business Continuity Planning sowie den Notfallplänen und deren Prüfung

Definition von IT bezogenen Notfallszenarien
auf Basis relevanter interner und externer Risiken

Vorbereitung auf mögliche Prüfungen
durch die Aufsichtsbehörde und Unterstützung bei der Dokumentenaufbereitung

Begleitung bei möglichen Prüfungen
Laufende Unterstützung während der Durchführung von aufsichtsrechtlichen Prüfungen

Nachbereitung möglicher Prüfungen
Unterstützung bei der Abarbeitung von aufgezeigten Feststellungen

Ihre Ansprechpartner

Mag. Alexander Ruzicka
Partner | Risk Advisory
+43 1 537 00-7950
aruzicka@deloitte.at

Mag. Thomas John
Senior Manager | Risk Advisory
+43 1 537 00-3723
tjohn@deloitte.at

www.deloitte.at/risk