Unternehmensberatung Dr.-Ing. Klaus-Rainer Müller
Am Roten Morgen 75, 64846 Groß-Zimmern

Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Marie-Curie-Str. 24-28
60439 Frankfurt

Unternehmensberatung
Dr.-Ing. Klaus-Rainer Müller

Freiberuflicher Ingenieur,
Referent und Fachautor
ISM, IRM, ITSCM, BCM

Am Roten Morgen 75
64846 Groß-Zimmern

Konsultation 14/2020 – MaRisk: Anregungen 03.12.2020

Sehr geehrte Damen und Herren,

Ihre Konsultation 14/2020 zur MaRisk habe ich mit Interesse gelesen. In Bezug auf meine Fachthemen möchte ich dazu Anregungen geben. Der schnelleren Erkennbarkeit wegen habe ich die Anregungen in roter Schrift gekennzeichnet.

Formulierung MaRisk	**Anregung**
AT 7.2 Technisch-organisatorische Ausstattung, Tz. 2, rechte Spalte	
Informationsverbund Zu einem Informationsverbund gehören bspw. geschäftsrelevante Informationen, Geschäfts- und Unterstützungsprozesse, IT-Systeme und die zugehörigen IT-Prozesse sowie Netz- und Gebäudeinfrastrukturen. **Standards zur Ausgestaltung der IT-Systeme** Zu solchen Standards zählen z. B. der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und die internationalen Sicherheitsstandards ISO/IEC 270XX der International Organization for Standardization.	**Informationsverbund** Zu einem Informationsverbund gehören bspw. geschäftsrelevante Informationen, Geschäfts- und Unterstützungsprozesse, IT-Systeme und die zugehörigen IT-Prozesse sowie Netz- und Gebäudeinfrastrukturen. Ebenfalls zum Informationsverbund gehören ausgelagerte IT-Services, wie bspw. Cloud-Computing-Services. **Standards zur Ausgestaltung der IT-Systeme und der IT-Prozesse** Zu solchen Standards zählen z. B. der IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI), die internationalen Standards zur Informationssicherheit der ISO/IEC-270XX-Familie der International Organization for Standardization sowie die Standards zum IT Service Management (ITSM) der ISO/IEC-20000-Reihe oder anerkannte gute Praktiken zum ITSM. *Grund der Anregung: Die MaRisk fordert auch für IT-Prozesse die Orientierung an Standards. Zudem enthalten die Standards der ISO/IEC-270xx-Familie Ausgestaltungshinweise für IT-Prozesse in Bezug auf Informationssicherheit.*

Formulierung MaRisk	Anregung
AT 7.3 Notfallmanagement, Tz. 1, rechte Spalte	
Auswirkungsanalysen In Auswirkungsanalysen (Business Impact Analysen) wird über abgestufte Zeiträume betrachtet, welche Folgen eine Beeinträchtigung von Aktivitäten und Prozessen für den Geschäftsbetrieb haben kann. Die Auswirkungsanalysen sollten u. a. folgende Aspekte berücksichtigen: - Art und Umfang des (im-)materiellen Schadens - Auswirkung des Zeitpunkts des Ausfalls auf den Schaden (z. B. Ausfall des Zahlungsverkehrs zu Hauptgeschäftszeiten)	**Auswirkungsanalysen** In Auswirkungsanalysen (Business Impact Analysen) wird über abgestufte Zeiträume betrachtet, welche Folgen eine Beeinträchtigung von Aktivitäten und Prozessen für den Geschäftsbetrieb haben kann. Die Auswirkungsanalysen sollten u. a. folgende Aspekte berücksichtigen: - Art und Umfang des (im-)materiellen Schadens - Auswirkung des Zeitpunkts des Ausfalls auf den Schaden (z. B. Ausfall des Zahlungsverkehrs zu Hauptgeschäftszeiten) Zu den möglichen Schadensarten gehören bspw. finanzielle Schäden, Reputationsschäden, Schäden durch Verstöße gegen gesetzliche, regulatorische und/oder vertragliche Anforderungen sowie Schäden durch Einschränkung der Handlungsfähigkeit. Der zeitliche Schadensverlauf in den Auswirkungsanalysen ist nachvollziehbar zu halten. Die Konsistenz der Ergebnisse der Auswirkungsanalysen ist sicherzustellen.
AT 7.3 Notfallmanagement, Tz. 1, rechte Spalte	
	Am Anfang der rechten Spalte könnte folgende Ergänzung aufgenommen werden: **Notfallmanagement** Orientierung für das Notfallmanagement und diesbezügliche Aufgabenstellungen können der internationale Standard zur Geschäftskontinuität ISO 22301 der International Organization for Standardization sowie weitere Standards dieser Familie geben. *Am Ende der rechten Spalte könnte folgende Ergänzung aufgenommen werden:* **Notfallstrategie** In der Notfallstrategie beschreibt das Institut die Optionen, die es zur Vermeidung, z. B. durch Redundanz, zur Erkennung und zur Behandlung der jeweiligen Notfallszenarien sowie zum Übergang in den Notbetrieb, zur Wiederherstellung und zur Rückkehr in den Normalbetrieb in Abhängigkeit vom Risiko wählt.

Formulierung MaRisk	Anregung
AT 9 Auslagerung, Tz. 2, rechte Spalte	
Risikoanalyse Bei der Risikoanalyse sind alle für das Institut relevanten Aspekte im Zusammenhang mit der Auslagerung zu berücksichtigen (z. B. … Risiken aus Weiterverlagerungen, politische Risiken, …	**Risikoanalyse** Bei der Risikoanalyse sind alle für das Institut relevanten Aspekte im Zusammenhang mit der Auslagerung zu berücksichtigen (z. B. … Risiken aus Weiterverlagerungen, politische Risiken, Risiken aufgrund des Rechtssystems, dem das Auslagerungsunternehmen sowie – sofern anwendbar – der Konzern unterliegt, zu dem es gehört, …
AT 9 Auslagerung, Tz. 7, rechte Spalte	
Informations- und Prüfungsrechte Informations- und Prüfungsrechte gem. Tz. 7 h) und i) sollten möglichst auch für nicht wesentliche Auslagerungen vereinbart werden, sofern abzusehen ist, dass diese Auslagerungen in naher oder mittlerer Zukunft wesentlich im Sinne der Tz. 2 werden könnten. Informations- und Prüfungsrechte gem. Tz. 7 h) und i) umfassen auch Zugangsrechte zu den für die ausgelagerten Prozesse und Aktivitäten relevanten Gebäuden des Auslagerungsunternehmens (z. B. Verwaltungsgebäude, Rechenzentren, Produktionsgebäude).	**Informations- und Prüfungsrechte** Informations- und Prüfungsrechte gem. Tz. 7 h) und i) sollten möglichst auch für nicht wesentliche Auslagerungen vereinbart werden, sofern abzusehen ist, dass diese Auslagerungen in naher oder mittlerer Zukunft wesentlich im Sinne der Tz. 2 werden könnten. Informations- und Prüfungsrechte gem. Tz. 7 h) und i) umfassen auch Zutrittsrechte zu den für die ausgelagerten Prozesse und Aktivitäten relevanten Gebäuden des Auslagerungsunternehmens (z. B. Verwaltungsgebäude, Rechenzentren, Produktionsgebäude). *Grund der Anregung: Durch optimierte Begrifflichkeiten sind Zutritt, Zugang und Zugriff leichter unterscheidbar, s.a. DIN EN 60839-11 zu elektronischen Zutrittskontrollanlagen.*

Freundliche Grüße sendet Ihnen

Dr.-Ing. Klaus-Rainer Müller