DORA….und was das an Nutzen und Aufwand bedeutet?

Einschätzungen aus der Begleitung laufender Projekte

Prof. Dr. Ralf Kühn, WP/CPA, Geschäftsführender Gesellschafter der Finance Audit GmbH Wirtschaftsprüfungsgesellschaft, Ettlingen

I. Hintergrund zu DORA

Der Finanzsektor, Banken wie Versicherungen, in Deutschland zeichnet sich bekanntlich bereits bisher durch eine intensive und mit durchaus hohem Prüfungsdruck „durchgesetzte" Regulatorik mit Bezug auf IT- und dienstleisterbezogene Themen aus. Dies gilt analog auch für eine Reihe anderer europäischer Länder – bei allerdings bestehenden großen nationalen Unterschieden in Schwerpunkten und Interpretation sowie in den Details des Ambitionsniveaus. Zugleich machen kritische Trends wie

- Klimawandel mit der damit verbundenen starken Zunahme von Extremwetterereignissen ohne relevante kurzfristige Besserungsperspektive,
- die kritische Sicherheitslage in Europa mit relevanten Gefahren des Übergangs in eine noch direktere Kriegsbeteiligung des Euroraums im Russland-Ukraine-Krieg und
- schlechte Arbeitsmarktlage in der Region D-A-CH mit akutem Arbeitskräfte- und Spezialistenmangel bei gleichzeitig hoher Jugendarbeitslosigkeit in vielen europäischen Ländern
- zahlreiche weitere globale Bedrohungen wie die globale dramatische Überbevölkerung

einen Bedrohungsrahmen, der aus Sicht der EU-Kommission eine weitere Erhöhung und Harmonisierung der IT-bezogenen Sicherheitsniveaus erfordert.

Das Gesetzgebungsverfahren für eine Verordnung über die digitale operationale Resilienz u.a. im Finanzsektor (sog. DORA-Verordnung) und anderen kritischen Industrien, die dies erreichen soll, wurde Ende 2022 abgeschlossen.
Am 14. Dezember 2022 unterzeichneten die Präsidenten des Rats und des Europäischen Parlaments den Verordnungstext, der aus einem Anfang 2021 eingeleiteten Trilogverfahren zwischen Kommission, Rat und Parlament hervorgegangen ist.
Die DORA-Verordnung wurde am 27. Dezember 2022 als Verordnung (EU) 2022/2254 und die sie begleitende Richtlinie als Richtlinie (EU) 2022/56 im Amtsblatt der Europäischen Union veröffentlicht.
Die DORA-Verordnung trat am 16. Januar 2023 (20 Tagen nach der Veröffentlichung) in Kraft und ist 24 Monate später anzuwenden.
Auch die Umsetzungsfrist für die Richtlinie endet am 17. Januar 2025.

Im 24-Monatszeitraum bis Anfang 2025 werden die in der DORA-Verordnung vorgesehenen Technischen Regulierungsstandards durch Entwürfe von den Europäischen Aufsichtsbehörden vorbereitet und später von der Kommission verabschiedet. Die erste Tranche dieser Technischen Regulierungsstandards wurde 2023 bereits veröffentlicht und befindet sich in Konsultation. Mit Blick auf die Überlagerungen von Inhalten der DORA-VO mit bestehenden aufsichtlichen Anforderungen hat die BaFin bereits in einem Beitrag der September-2022-Ausgabe des BaFin-Journals angekündigt, die bestehenden Rundschreiben (BAIT, VAIT, KAIT, ZAIT) perspektivisch zu überarbeiten, um sicherzustellen, dass „keine regulatorische[n] Dopplungen entstehen". Partiell waren bereits in den BAIT 2021 einzelne Aspekte vorweggenommen worden.

Mit der DORA-Verordnung und diesen Technischen Regulierungsstandards verfolgt die Europäische Kommission explizit das Ziel, einen einheitlichen Rahmen für ein effektives und umfassendes Management von Cybersicherheits- und IKT-Risiken auf den Finanzmärkten zu schaffen.
Dabei wird - auf Basis der oben dargestellten Gefährdungsanalyse zweifellos konsequent und richtig - der Schwerpunkt von der Gewährleistung der finanziellen Widerstandsfähigkeit von Finanzunternehmen partiell erweitert auf die Sicherstellung der Aufrechterhaltung eines widerstandsfähigen Betriebs im Falle einer schwerwiegenden Betriebsunterbrechung, die die Sicherheit des Netzes und der Informationssysteme gefährden könnte. Durch steigende Cyberangriffe ist es für Finanzunternehmen notwendiger denn je, sich auf Vorfälle vorzubereiten und Maßnahmen zur Stärkung der Cyber-Resilienz einzuführen. Es ist, so die EU-Kommission, mit Anpassungen und Mehraufwänden zu rechnen – die die EU bewusst in Kauf nimmt. Sie sieht DORA gleichzeitig als große Chance für Finanzunternehmen, durch eine gestärkte Resilienz und einen konsistenten Reifegrad in Sachen Cybersicherheit zu einem signifikant höheren Sicherheitsniveau aufzusteigen und damit das eigene Überleben der jeweiligen Finanzunternehmen auch unter neuer Bedrohungslage zu gewährleisten. Anders formuliert: Wer DORA nicht erfüllt, ist aus Sicht der EU-Kommission der derzeitigen Bedrohungslage nicht nachhaltig gewachsen und nicht nachhaltig überlebensfähig…..was wenig Raum für regulatorische Kompromisse und Proportionalitätsüberlegungen lässt. Dies ist – das kann aus Sicht des Autors mit nun über 30 Jahren Erfahrung als Prüfer und Berater, auch als Prüfer in finanzaufsichtlichen Sonderprüfungen, nicht genug hervorgehoben werden, da es allen Beteiligten wenig Spielraum für regulatorische Kompromisse lässt.

Ziel der BAIT/VAIT/ZAIT/KAIT waren ja insbesondere die Einhaltung der Angemessenheit und Funktionsfähigkeit in den Themen

- IT-Strategie
- IT-Governance
- Informationsrisikomanagement
- Informationssicherheitsmanagement
- Operative Informationssicherheit
- Identitäts- und Rechtemanagement
- IT-Projektmanagement
- Anwendungsentwicklung inklusive der Anforderungen an die individuelle Datenverarbeitung (IDV)
- IT-Betrieb
- Business Continuity Management inkl. IT-Notfallmanagement/ IT-Service Continuity Management
- Auslagerungen/ Ausgliederungen von IT-Dienstleistungen und sonstige Dienstleistungsbeziehungen im Bereich IT-Dienstleistungen inkl. Cloud-Services.

Diese zielten u.a. auch auf ein komplexes und gut organisiertes Zusammenwirken verschiedenster Rollen und Prozesse bezüglich

- Effizienz und Effektivität des arbeitsteiligen Zusammenwirkens der verschiedenen Rollen
- Methodisches Alignment der jeweiligen Ansätze
- Proaktives “Leben” eines 3-Lines-of-Defense-Modells
- qualitative und quantitative Personalausstattung
- Aktives und systematisch geplantes Kontrollhandeln mit entsprechender Berichterstattung und Follow-up

- unter Wahrung der Funktionstrennung zu den operativen Linieneinheiten

Unbeschadet der Relevanz aller genannten Aspekte und der Tatsache, dass wesentliche oder schwerwiegende Feststellungen in den meisten dieser Themenfelder nicht nur denkbar sind, sondern auch regelmäßig vorkommen, sind es derzeit vor allem die folgenden Punkte, die in aufsichtlichen Prüfungen zu BAIT/VAIT/ZAIT/KAIT besonders im Fokus stehen:

- ➔ Praxistauglichkeit und Realitätsnähe der Notfallvorsorge und der Maßnahmen im Bereich des operativen Informationssicherheit
- ➔ Hohe Anforderungen an die zeitliche Taktung und den Abdeckungsgrad dieser Maßnahmen (Vollständigkeit auf System- und Szenarioebene)
- ➔ Szenarien politisch-terroristischer Cyberangriffe sind konsequent abzudecken
- ➔ SIEM-Systeme und andere Systeme zu regelbasierten und zeitnahen Überwachung sowie Schnelligkeit der Reaktion auf so erkannte potenzielle Auffälligkeiten stehen unter hohem Erwartungs- und Umsetzungsdruck
- ➔ Besondere Betonung des 3-Lines-of-Defense-Modells
- ➔ „Security Operation Center“ und damit 7*24-Reaktion als Standard der Informationssicherheit
- ➔ Schwachstellenscans, Penetrationstests und andere präventive Maßnahmen der Schwachstellenidentifikation und -bereinigung sind konsequent zu implementieren.
- ➔ Programmhafte, strukturierte Schulungen zur Informationssicherheit und Vorgaben der 2nd Line dafür sowie das „Awareness-Testing“ als Erfolgskontrolle

Zu zwei dieser Schwerpunkte führen wir das nachfolgend noch etwas detaillierter aus.

II. Schwerpunkte der Neuerungen durch DORA

DORA umfasst zwar prinzipiell alle auch durch BAIT/VAIT/KAIT/ZAIT adressierten IT-bezogenen Themen- aber eben doch in einer deutlich risikoorientierteren und auf die „Meta-Cyber-Bedrohungen“ ausgerichteten Art und Weise.
Daher stehen die folgenden Themen und Schwerpunkte in DORA im Vordergrund:

Operational Resilience und Risikomanagement
Finanzunternehmen sind verpflichtet, ein umfassendes IKT-Risikomanagement einzurichten, einschließlich

- Einrichtung und Pflege belastbarer IKT-Systeme und -Werkzeuge, die die Auswirkungen von IKT-Risiken minimieren,
- Schlüsselelemente wie Identifizierung, Klassifizierung und Dokumentation kritischer Funktionen,
- Kontinuierliche Überwachung aller Quellen von IKT-Risiken, um Schutz- und Präventionsmaßnahmen einzurichten,
- Sofortige Erkennung von anomalen Aktivitäten,
- Einführung spezieller und umfassender Business-Continuity-Richtlinien sowie Notfall- und Wiederherstellungspläne, einschließlich jährlicher Tests der Pläne, die alle unterstützenden Funktionen abdecken,
- Einrichtung von Mechanismen, um sowohl aus externen Ereignissen als auch aus eigenen IKT-Vorfällen zu lernen und sich weiterzuentwickeln.

Management von IKT-Vorfällen und Cyber Security

Finanzunternehmen sind verpflichtet:

- ein wirksames Verfahren zu entwickeln, um alle IKT-Vorfälle zu protokollieren/zu klassifizieren und schwerwiegende Vorfälle gemäß den in der Verordnung aufgeführten und von den europäischen Aufsichtsbehörden (EBA, EIOPA und ESMA) weiter spezifizierten Kriterien zu bestimmen,
- einen Anfangs-, Zwischen- und Abschlussbericht über IKT-bezogene Vorfälle vorzulegen,
- die Berichterstattung über IKT-bezogene Vorfälle anhand der von den ESAs entwickelten Standardvorlagen zu harmonisieren.

Digital Operational Resilience Testing

Die Verordnung verpflichtet alle Einrichtungen, dass sie

- jährlich grundlegende Tests von IKT-Werkzeugen und -Systemen durchführen,
- Schwachstellen, Mängel oder Lücken identifizieren, abmildern und umgehend beseitigen, indem sie Gegenmaßnahmen ergreifen,
- regelmäßig fortgeschrittene bedrohungsgesteuerte Penetrationstests (TLPT) für IKT-Dienste durchführen, die sich auf kritische Funktionen auswirken. Drittanbieter von IKT-Dienstleistungen sind verpflichtet, an den Tests teilzunehmen und vollständig zu kooperieren.

Governance und Management von Drittparteien

Die Finanzunternehmen sind verpflichtet:

- eine solide Überwachung der Risiken zu gewährleisten, die sich aus der Inanspruchnahme von IKT-Drittanbietern ergeben,
- ein vollständiges Verzeichnis aller ausgelagerten Tätigkeiten, einschließlich gruppeninterner Dienstleistungen und aller Änderungen bei der Auslagerung kritischer Dienstleistungen an IKT-Drittanbieter, zu melden,
- das IT-Konzentrationsrisiko und die Risiken, die sich aus Sub-Outsourcing-Aktivitäten ergeben, zu berücksichtigen,
- Schlüsselelemente der Dienstleistung und der Beziehung zu IKT-Drittanbietern zu harmonisieren, um eine „vollständige“ Überwachung zu ermöglichen,
- sicherzustellen, dass die Verträge mit den IKT-Drittanbietern alle notwendigen Details zur Überwachung und Erreichbarkeit enthalten, wie z. B. eine vollständige Beschreibung des Leistungsumfangs, die Angabe der Standorte, an denen die Daten verarbeitet werden, usw.,
- Kritische IKT-Drittdienstleister werden einem EU-Aufsichtsrahmen unterliegen, der Empfehlungen zur Minderung festgestellter IKT-Risiken aussprechen kann. Finanzunternehmen müssen die IKT-Drittrisiken ihres Dienstleisters berücksichtigen, wenn dieser die festgelegten Empfehlungen nicht befolgt.

Informationsaustausch

- Die Verordnung erlaubt es Finanzunternehmen, untereinander Vereinbarungen zum Austausch von Informationen und Erkenntnissen über Cyberbedrohungen zu treffen.
- Die Aufsichtsbehörde wird den Finanzunternehmen relevante anonymisierte Informationen und Erkenntnisse über Cyber-Bedrohungen zur Verfügung stellen. Daher sollten die Unternehmen Mechanismen einrichten, um die von den Behörden weitergegebenen Informationen zu überprüfen und entsprechende Maßnahmen zu ergreifen.

Liest man diese Schwerpunkte, so fallen folgende Punkte ins Auge, die zugleich den praktischen Rahmen für entsprechende DORA-Umsetzungsprojekte in Finanzunternehmen setzen sollten:

- Für Finanzunternehmen, die bereits BAIT/VAIT/KAIT/ZAIT umzusetzen hatten, ergibt sich auf der „Überschriftenebene“ zunächst keine völlig neue Themenstellung

aber:

- Viele aufsichtliche Prüfungen zeigen bekanntlich, dass viele Finanzunternehmen auch die bestehende Regulatorik zu BAIT/VAIT/KAIT/ZAIT nicht auf dem von den aufsichtlichen Prüfungen geforderten Niveau umgesetzt haben. Hier gilt es, mit entsprechender Konsequenz zunächst diese bestehenden Umsetzungslücken zu schließen. Erste Erfahrungen aus der Begleitung konkreter Projekte zeigen, dass DORA-Anforderungen auf keinen Fall neben BAIT/VAIT/KAIT/ZAIT-Projekten, sondern als ein integriertes Projekt umgesetzt werden sollten, um methodische Inkonsistenzen, Mehrfachaufwände und Akzeptanzprobleme der Fachbereiche angesichts ohnehin sehr hoher Umsetzungsdrucke in verschiedenen Themenfeldern zu vermeiden und eine pragmatische Umsetzung so effizient und effektiv wie möglich zu gewährleisten.
- DORA erhöht in einer Reihe von Feldern das fachliche und zeitliche Ambitionsniveau deutlich, d.h. die zu „überspringende Hürde“ wird höher, der technologische Reifegrad muss steigen, ebenso die Prozessautomatisierung in den DORA-Gebieten.
- Über verschiedene Meldeprozesse stehen auch den Regulatoren deutlich erweiterte Daten zur Verfügung, die es erlauben, erweiterte Rückschlüsse über den Umsetzungsreifegrad in Finanzunternehmen zu ziehen.

Damit bleibt festzuhalten, dass auch ein Abwarten und „Aussitzen“ von DORA ausscheidet. Nur, wer sich jetzt systematisch und im Sinne klarer GAP-Betrachtungen sowohl mit seinem Status zu BAIT/VAIT/KAIT/ZAIT als auch mit DORA beschäftigt und die entsprechenden Umsetzungen systematisch organisiert angeht, kann erwarten, je nach „Absprungpunkt“ entweder pünktlich 2025 oder doch zumindest 2026/2027 den nötigen Umsetzungsstand einigermaßen zu erreichen. Dabei sei verdeutlicht: Angesichts der Dynamik und Komplexität der dahinter stehenden Herausforderungen kann es hierbei nicht darum gehen, „Musterschüler“ zu sein oder durch dokumentatorisches „Schaulaufen“ reale Strukturen und Prozesse zu verdecken, sondern effektiv und effiziente

- Systeme,
- Prozesse und
- Strukturen zu schaffen,

in denen

- agile
- kompetente
- kostenbezogen tragfähige
- dokumentierte
- handlungs- und entscheidungsorientierte
- praxiserprobte
- präventiv wie detektiv ausgerichtete
- selbstlernende
- regelbasierte
- durch Technik state-of-the.art unterstützte

Sicherheitsarchitekturen etabliert und wirksam sind.

Nachfolgend sei dies an einem der DORA-Schwerpunkte exemplarisch erläutert – hier aus dem Kontext „Operational Resilience“:

III. Schwerpunkte von DORA im Kontext des Business Continuity Managements/ IT-Service-Continuity-Managements

1. Erwartungen an den Prozess

DORA beinhaltet hier insbesondere:

- die Zielsetzung / den Rahmen für das Notfallmanagement,
- die Definitionen und die Beschreibung des Notfallvorsorgekonzepts,
- die Festlegung der Notfallorganisation,
- die gesamte Umsetzung der Notfallvorsorge in Plänen, Tests und Übungen und
- die Regelungen zur Sensibilisierung der Mitarbeiter.

Danach ist für Notfälle bei allen zeitkritischen Aktivitäten und Prozessen im Rahmen der regulatorischen Vorgaben und des zu formulierenden Risikoappetits sowie einer szenariobasierten Analyse möglicher Bedrohungen der jeweiligen Institution Notfallvorsorge zu treffen. Aus diesem Grund hat sich die Geschäftsführung des Unternehmens dazu zu bekennen, ein Notfallmanagement-System / Business Continuity Management-System im Unternehmen zu etablieren sowie dauerhaft zu betreiben und zu verbessern.
Das BCM / Notfallmanagement sollte sich hierzu an einer Internationalen Norm, z.B. DIN:EN ISO 22301, zu orientieren.

Zur Erreichung dieser Zielsetzung müssen für identifizierte Notfallszenarien, zu denen auch die DORA zu Grunde liegenden Notfallszenarien gehören müssen - und für zeitkritische Geschäftsprozesse Geschäftsfortführungs- sowie Wiederanlaufpläne und szenariobasierte Notfallpläne definiert werden, deren Durchführbarkeit im Rahmen von regelmäßigen Notfalltests sichergestellt werden muss. Hauptziel des BCM ist es, für die identifizierten kritischen Geschäftsprozesse und Szenarien den Geschäftsbetrieb in der für den Notfall erforderlichen Form und Zeit sicherzustellen und hinreichende Vorsorge für den Wiederanlauf der Regelprozesse zu betreiben und damit das Überleben des Finanzunternehmens und seiner Hauptleistungen als kritische Infrastruktur zu gewährleisten.

Die eigentliche Verantwortung des BCM/Notfallmanagements besteht dabei in der Sicherstellung von Resilienz und Reaktionsfähigkeit des Gesamtunternehmens bei Notfällen oder sich abzeichnenden Notfällen. Es gelten insbesondere folgende Maßstäbe:

- Für alle zeitkritischen Geschäftsprozesse existiert eine Notfallplanung für den Notbetrieb. Dabei werden die relevanten Ressourcen (z.B. Informationen, Anwendungen, Mitarbeiter, Lokationen, Dienstleister) zwingend berücksichtigt.
- Das BCM / Notfallmanagement muss die Aufrechterhaltung der zeitkritischen Geschäftsprozesse auch in außergewöhnlichen, planbaren Situationen wie z.B. regionalen Naturkatastrophen gewährleisten.
- Die Maßnahmen müssen geeignet sein, um nachhaltige Reputationsschäden durch einen Notfall zu vermeiden. Hierzu sind geeignete Kommunikationswege in den Notfallkonzepten vorzusehen.

- Die Notfallkonzepte und Wiederanlaufpläne müssen geeignet sein, die gesetzlichen und aufsichtsrechtlichen Anforderungen zu erfüllen, d.h. Gesetzesverstöße dürfen auch für den Notfall nicht eingeplant/ akzeptiert werden.
- Zur Wirksamkeit und Angemessenheit der Notfallpläne und stetigen Verbesserung sind regelmäßige und praxisnahe Notfallübungen und Echttests durchzuführen. Deren Befunde fließen qualitätssichernd wieder in das Notfallmanagement ein. Dies gilt auch für die Erkenntnisse aus echten Notfällen. Turnus, Inhalt und Umfang der Notfallübungen richten sich neben den betrieblichen Anforderungen auch nach den gesetzlichen und regulatorischen Anforderungen der MaRisk 2021 und BAIT 2021.
- Die Unternehmensleitung ist grundsätzlich für das Notfallmanagement verantwortlich (siehe § 25a Abs. 1 Nr. 5 KWG).
- Zur Kontrolle und Steuerung des Notfallmanagements berichtet der Notfallbeauftragte regelmäßig an die Geschäftsleitung, die den nötigen „Tone-from-the-Top“ setzt.

2. Erwartungen an die Notfallorganisation

Im Rahmen des BCM unterhält das Unternehmen eine Notfallorganisation. Diese besteht aus:
- einer Notfallvorsorgeorganisation
- und einer Notfallbewältigungsorganisation.

Die für die Feststellung der Kritikalität als Maßstab der maximal anzustrebenden Ausfallzeiten erforderliche Methodik ist eindeutig zu beschreiben.

Das Finanzunternehmen leitet aus der mindestens jährlich durchzuführenden Prozessklassifizierung im Rahmen einer Business Impact Analyse und weitergehenden Risk Impact Analysen im Zusammenhang mit der damit einhergehenden Schutzbedarfs- und Kritikalitätseinschätzung die Relevanz der im Notfallmanagement zu betrachtenden Prozesse ab. Über eine Risk Impact Analyse wird validiert, welche Risikoszenarien für diese Prozesse wie unter Absicherungsaspekten zu berücksichtigen sind. Den Fachbereichen obliegt dabei sowohl die Festlegung des Schutzbedarfs im Normalbetrieb als auch im Notbetrieb (Kritikalität). Die Einstufung der Werte je bewertetem Kriterium erfolgt auf Basis einer Experteneinschätzung, die durch quantitativ und qualitativ aussagekräftige Begründungen so zu unterlegen ist, dass sie durch einen sachkundigen Dritten nachvollzogen werden kann.

Aufgabe des Notfallmanagements ist die Notfallorganisation sowie die Implementierung, Steuerung, Durchführung, Überwachung und Weiterentwicklung von Maßnahmen und Plänen, die zur Fortführung der zeitkritischen Geschäftsprozesse auf Basis der jeweiligen maximal tolerierbaren Ausfallzeit (MTA) erforderlich sind. Diese sind ausreichend konkret, aber zugleich auch mit der nötigen Reaktionsfähigkeit auf das in Notfällen zwingend dynamische und teils nicht vorhersehbare äußere Geschehen auszugestalten. Das Ziel wird abgesichert durch die im Rahmen des Notfallmanagement auf Grundlage einer Business Impact Analyse (BIA) zu entwickelnden Geschäftsfortführungs-, Wiederanlauf- und szenarienbasierten Notfallpläne. Hierzu ist auch die Sicherstellung aufeinander abgestimmter Notfallkonzepte mit externen Dienstleistern, die (Teil-)Leistungen für zeitkritische Prozesse der Bank erbringen, zwingend erforderlich – inklusive der entsprechenden vertraglichen Absicherung.

Der Notfallprozess unterliegt zwingend dem folgenden Zyklus:
- Planung von Maßnahmen

- Umsetzen dieser Maßnahmen
- Überwachung und Prüfung der Maßnahmen
- Verbesserung der Maßnahmen

Auf der Basis einer systematischen und wiederkehrenden Analyse aller Prozesse sind die „zeitkritischen“ Prozesse zu identifizieren. Für diese sind Maßnahmen zur Minimierung der Auswirkungen potentieller Schadenfälle zu definieren (z. B. Geschäftsfortführungs- und Wiederanlaufpläne).

Zur Basisabsicherung sind mindestens folgende Szenarien zu betrachten:

- Szenario 1
  (Teil-)Ausfall Hauptgebäude (zum Beispiel Zerstörung durch Brand) inklusive Versorgungsausfall (Strom/Wasser etc.)
- Szenario 2
  Ausfall der IT bzw. der Informationsversorgung über einen längeren Zeitraum (zum Beispiel Ausfall einer Serverbereitstellungsfläche) inklusive Ausfall Telekommunikation und Ausfall Netzwerk, auch im Fall von Cyberangriffen oder schwerwiegenden Sicherheits-/Informationssicherheitsvorfällen
- Szenario 3
  Ausfall von notfallrelevanten Dienstleistern (zum Beispiel System-/ Serverausfall bei einem zentralen IT-Dienstleister), ob Auslagerung oder sonstiger (IT-)Fremdbezug
- Szenario 4
  Ausfall von Personal (zum Beispiel Ausfall der Mitarbeiter wegen Pandemie)

Dabei ist es nicht zulässig, aufgrund von bestehenden vertraglichen Vereinbarungen und fehlender Negativerfahrungen in der Vergangenheit „automatisch“ davon auszugehen, dass ein Dienstleister keine Ausfallzeiten länger als die vertraglich zugesicherten Analyse- und Wiederanlaufzeiten haben kann.

Insbesondere ist sicherzustellen, dass folgende Aufgaben umgesetzt werden:

- Überwachung der Einhaltung gesetzlicher Vorschriften und Standards zur Notfallvorsorge
- Pflege des übergreifenden Notfallhandbuchs
- Festlegung und Prüfung der durch Fachbereiche zu erstellenden Notfallpläne (z.B. IT, Gebäude, Personal)
- Planung der Notfallkonzeption
- Festlegung und Dokumentation der Methodik zur zeitlichen Schadensanalyse, Kritikalitätseinstufung, Business-Impact-Analyse (BIA)
- Priorisierung der Geschäftsprozesse anhand ihrer Kritikalität und ihres zeitlichen Schadensverlaufs
- Initiierung der Durchführung der BIA und Erstellung der Geschäftsfortführungspläne (Notbetriebsbeschreibungen)
- Erstellung von Notfallplänen, mindestens zu den Notfallszenarien Ausfall IT und Informationsversorgung, Gebäudeausfall, Ausfall Personal und Ausfall relevanter Dienstleister
- Pflege und Fortführung der Geschäftsfortführungs- und Notfallpläne
- Umsetzung von begleitenden Notfallvorsorgemaßnahmen
- Erstellung übergreifende Notfallübungsplanung
- Planung, Durchführung und Dokumentation von Notfallübungen

- Definition und Bewertung von Maßnahmen nach Notfallübungen
- Steuerung und Kontrolle der Maßnahmenumsetzung
- Regelmäßige (mindestens einmal pro Jahr / vierteljährlich) und anlassbezogene Berichterstattung an die Unternehmensführung
- Regelmäßige Abstimmung mit weiteren Funktionsträgern und Organisationsbereichen, wie z. B: Informationssicherheits-Beauftragter, Brandschutzbeauftragter, Sicherheitsbeauftragter, Manager operationelle Risiken, Risikocontrolling, Dienstleistersteuerung, Mitglieder des Krisenstabes, Verantwortliche von Prozessen und Anwendungen, übergreifendes Prozessmanagement
- Erstellung und Pflege eines Sensibilisierungs- / Schulungs-konzepts

PRAXISTIPPS

- Führen Sie auch bei DORA keine “Alibi”-Diskussionen, sondern treffen Sie materiell und regulatorisch gut abgewogene Managemententscheidungen.
- Versuchen Sie nicht, im ersten “Anlauf” perfekte Lösungen zu finden, sondern setzen Sie bewusste Reifegradstufen um.
- Geänderte Bedrohungslagen müssen auch zu entsprechenden operativen Maßnahmen führen, d.h. Hintergrund jeder DORA-bezogenen Entscheidung sollte ihre Bedrohungs- und Gefährdungsanalyse sein.
- Angesichts geänderter Bedrohungslage sind rein vergangenheitsbezogene Sichtweisen („bisher ist dazu auch nichts passiert“) ebenso deplatziert wie „Panikmache“ („DORA verändert alles“- „nein, tut es nicht“, aber DORA entwickelt bestehende Anforderungen dynamisch weiter).
- Wenn es um materielle Sicherheitsniveau geht, sind Proportionalitätsdiskussionen fehl am Platz, anders als bei Dokumentationsanforderungen.
- Bei allen Anforderungen im Detail: verlieren Sie nicht den Blick für den “unternehmerischen Menschenverstand”, wenn Sie DORA umsetzen wollen.