Institut für Business Continuity & Resilience Management e.V. - Postfach 21 01 71 - 50527 Köln

Bundesanstalt für Finanzdienstleistungsaufsicht
Marie-Curie-Str. 24-28
60439 Frankfurt am Main

Stellungnahme zum Konsultationsverfahren 14/2020 – Mindestanforderungen an das Risikomanagement

Sehr geehrter Herr Röseler,

als das führende nationale Fachinstitut für Business Continuity & Resilience Management in Deutschland machen wir es uns zur Aufgabe, u.a. das Thema Notfallmanagement für alle Interessengruppen der deutschen Wirtschaft zu positionieren, zu fördern und weiterzuentwickeln.

Vor diesem Hintergrund nehmen wir im Rahmen des Konsultationsverfahrens 14/2020 – Mindestanforderungen an das Risikomanagement vom 26. Oktober 2020 Stellung.

Im Folgenden finden Sie unsere Stellungnahme.

AT 7.3 Notfallkonzept - 1

Das Institut hat Ziele zum Notfallmanagement zu definieren und hieraus abgeleitet einen Notfallmanagementprozess festzulegen. Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. ~~Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen. Die Ergebnisse der Notfalltests sind den jeweiligen Verantwortlichen mitzuteilen. Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte zu verfügen.~~ Das Notfallkonzept ist anlassbezogen zu aktualisieren, jährlich auf Aktualität zu überprüfen und angemessen zu kommunizieren. Die Geschäftsleitung hat sich mindestens quartalsweise und anlassbezogen über den Zustand des Notfallmanagements schriftlich berichten zu lassen.

Zeitkritische Aktivitäten und Prozesse
Zeitkritisch sind grundsätzlich jene Aktivitäten und Prozesse, bei deren Beeinträchtigung für definierte Zeiträume ein nicht mehr akzeptabler Schaden für das Institut zu erwarten ist.

Zur Identifikation von zeitkritischen Aktivitäten und Prozessen sowie von unterstützenden Aktivitäten und Prozessen, hierfür notwendigen IT-Systemen und sonstigen notwendigen Ressourcen sowie den potentiellen Gefährdungen führt das Institut Auswirkungsanalysen und Risikoanalysen durch. Als Basis hierfür dient eine Übersicht über alle Aktivitäten und Prozesse (z. B. in Form einer Prozesslandkarte).

Auswirkungsanalysen
In Auswirkungsanalysen (Business Impact Analysen) wird über abgestufte Zeiträume betrachtet, welche Folgen eine Beeinträchtigung von Aktivitäten und Prozessen für den Geschäftsbetrieb haben kann.

Institut für Business Continuity & Resilience Management e.V.

1. Vorstand: Franziska Hain
2. Vorstand: Sandra Achilles

Adresse Postfach 21 01 71
50527 Köln
Email info@ibcrm.de
Webseite www.ibcrm.de

Bank Kreissparkasse Köln (KSK)
BIC COKSDE33XXX
IBAN DE13 3705 0299 0012 008 003
VR-Nr. 19274 Amtsgericht Köln
Steuernummer 220 5992 1872

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)

Risikoanalysen
In Risikoanalysen (Risk Impact Analysen) für die identifizierten zeitkritischen Aktivitäten und Prozesse werden potentielle Gefährdungen identifiziert und bewertet, welche eine Beeinträchtigung der zeitkritischen Geschäftsprozesse verursachen können.

Änderungs-/Ergänzungsvorschlag des IBCRM e.V.

Das Institut hat Ziele zum Notfallmanagement zu definieren und ~~hieraus abgeleitet~~ **einen** ~~Notfallmanagement~~Prozess **für das betriebliche Kontinuitätsmanagement** ~~festzulegen~~ **auf Basis einer von der Unternehmensleitung freizugebenden Leitlinie** zu etablieren.

...führt das Institut **regelmäßig und anlassbezogen** Auswirkungsanalysen und Risikoanalysen durch..

Als Basis hierfür ~~dient eine Übersicht~~ **dienen strukturierte Übersichten** über alle Aktivitäten und Prozesse (z. B. in Form einer Prozesslandkarte) **und die jeweiligen unterstützenden bzw. erforderlichen Ressourcen (z. B. in Form einer CMDB für die IT-Systeme, IT-Anwendungen und ggf. Hardware).**

Erläuterung, Hinweise und Fragen des IBCRM e.V.

Ziele des Notfallmanagements
Wir empfehlen in der Anforderung deutlich zu machen, dass die Zielvorgabe für ein Notfallmanagement durch die Unternehmensleitung vorzunehmen und mittels einer Leitlinie umzusetzen ist.

Die Formulierung ".. hieraus abgeleitet einen Notfallmanagementprozess festzulegen" empfehlen wir zu überarbeiten. Der Prozess sollte nicht zwangsweise aus den Zielen des Notfallmanagements selbst "abgeleitet" sein, deren Erreichung jedoch realisieren.

Betrieblicher Prozess
Wir empfehlen die Verwendung des „betrieblichen Kontinuitätsmanagements“ anstelle des Begriffs „Notfallmanagement“.

In der betrieblichen Praxis wird häufig das Notfallmanagement als Prozess in der Reaktion auf eine disruptive Situation verstanden, dessen Aktivitäten auf die Steuerung des Ereignisses selbst ausgerichtet sind. Die Ursache für dieses Verständnis sehen wir in der häufig angewendeten Differenzierung zwischen einem 1) Notfall und einer 2) Krise, welche in Folge die Etablierung eines 1) Notfallmanagements und eines davon losgelösten 2) Krisenmanagements zur Folge hat.
(Im Übrigen erfolgt in diesen Fällen wiederrum die Umsetzung meist dann nicht trennscharf, wenn es z.B. um personelle Kapazitäten geht. Auf dem Papier wird zwischen dem Notfallteam und dem Krisenteam unterschieden, de facto handelt es sich jedoch oft um die gleichen Personen.)
Wir empfehlen im Mindesten bei der Verwendung des Begriffs "Notfallmanagementprozess" den Hinweis aufzunehmen, dass darunter das betriebliche Kontinuitätsmanagement gemeint sei. Damit wäre klargestellt,

dass es sich insbesondere um den Prozess zur Erarbeitung der präventiven Absicherung geht und Elemente wie die Umsetzung einer Auswirkungsanalyse und die Erarbeitung von Geschäftsfortführungs-/Wiederanlaufplänen handelt.
Zudem gibt es noch immer Handlungs-/Regulierungsbedarf, das Thema Notfallmanagement nachhaltiger in den Instituten zu etablieren. Idealer Weise sollte daher die Umsetzung innerhalb eines Zyklus-Models (BIA, RIA, NFK, Tests/Überprüfungen, Verbesserungen und wiederkehrend ablaufend) synchronisiert mit dem Plan-Do-Check-Act Ansatz wie in der ISO 22301/22313 gefordert werden.

Leitlinie

Dieses strategische Dokument gibt den aufbauorganisatorischen Rahmen inklusive der Rollen und Verantwortlichkeiten sowie die Inhalte des betrieblichen Prozesses vor und sollte unseres Erachtens nach Einzug in die Anforderungen des AT 7.3 (1) halten.

Zyklus

Einhergehend sollte außerdem explizit geregelt werden, ob dieser Zyklus innerhalb eines Jahres oder eines selbst gewählten Zeitraums absolviert werden muss. Im Zusammenhang mit der Forderung nach jährlicher Aktualisierung und jährlicher Überprüfung der Wirksamkeit der Notfallkonzepte für alle "relevanten" Szenarien für zeitkritische Aktivitäten und Prozesse (AT 7.3 (3)) scheint diese Vorgabe indirekt schon existent zu sein und daher in der Prüfpraxis Missverständnisse vermeidend genannt werden.

Übersichten

Wir empfehlen weiterhin die Ressourcen-Sicht in die geforderte Übersicht aufzunehmen, da Ressourcen aufgrund ihrer heterogenen Quellen sowie einer mangelnden Dokumentation oftmals nicht in ihrer Vollständigkeit einbezogen werden.

Risikoanalysen

Es ist regelmäßig unklar, welchen Umfang die Risikoanalyse innerhalb des betrieblichen Kontinuitätsmanagements ausmacht, zumal die Auswirkungsanalyse ebenso Elemente einer Risikoanalyse aufweist (wenn auch in sehr spezieller Form). Hier schlagen wir eine Abgrenzung zwischen den jeweiligen Risikoperspektiven anhand folgender Fragestellungen vor:

1. Welche (Krisen-)Szenarien sind für das Institut von Bedeutung und bedürfen aufgrund von entsprechenden Eintrittswahrscheinlichkeiten einer Absicherung? (Diese Risikobetrachtung i.S. einer (Ausfall-)Szenario-Analyse ist Teil des Notfallmanagementprozesses.)
2. Welchen Gefährdungen unterliegen die Ressourcen des Normalbetriebs und können bei Eintritt den Ablauf der zeitkritischen Aktivitäten bedeutsam (außerhalb eines tolerablen Schadens) beeinflussen? (Diese Risikobetrachtung liegt eher außerhalb des Notfallmanagementprozesses.)
3. Welchen Gefährdungen unterliegen Ressourcen, die im Not-/Krisenfall zum Einsatz kommen und bei Eintritt einer Gefährdung den Ablauf der zeitkritischen Aktivitäten in A) der Geschäftsfortführung (inkl. Notbetrieb) und B) der Wiederherstellung bereits im geringen Maß beeinflussen? (Diese Risikobetrachtung ist Teil des Notfallmanagementprozesses.)

AT 7.3 Notfallkonzept – 2

Das Notfallkonzept muss Geschäftsfortführungs- sowie Wiederherstellungspläne ~~Wiederanlaufpläne~~ umfassen. ~~Die~~ Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung

stehen. ~~Die~~ Wiederherstellungspläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen.
Bei Notfällen ist eine angemessene interne und externe Kommunikation sicherzustellen. Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte zu verfügen. ~~Die im Notfall zu verwendenden Kommunikationswege sind festzulegen. Das Notfallkonzept muss den beteiligten Mitarbeitern zur Verfügung stehen.~~

Notfallkonzept
Im Notfallkonzept werden Verantwortlichkeiten, Ziele und Maßnahmen zur Fortführung bzw. Wiederherstellung von zeitkritischen Aktivitäten und Prozessen bestimmt und Kriterien für die Einstufung sowie für das Auslösen der Pläne definiert.

Notfallszenarien
Hierbei werden mindestens folgende Szenarien berücksichtigt:
- (Teil-)Ausfall eines Standortes (z. B. durch Hochwasser, Großbrand, Gebietssperrung, Ausfall der Zutrittskontrolle)
- Erheblicher Ausfall von IT-Systemen oder Kommunikationsinfrastruktur (z. B. aufgrund von Fehlern oder Angriffen)
- Ausfall einer kritischen Anzahl von Mitarbeitern (z. B. bei Pandemie, Lebensmittelvergiftung, Streik)
- Ausfall von Dienstleistern (z. B. Zulieferer, Stromversorger)

Änderungs-/Ergänzungsvorschlag des IBCRM e.V.

Geschäftsfortführungspläne müssen gewährleisten, dass im Notfall zeitnah Ersatzlösungen zur Verfügung stehen **und beschreiben, welche Änderungen an den Arbeitsabläufen als Reaktion auf ein zugrunde gelegtes Szenario möglich sind**.

Wiederherstellungspläne müssen innerhalb eines angemessenen Zeitraums die Rückkehr zum Normalbetrieb ermöglichen **und Regelungen enthalten, wie Arbeitsrückstände (Backlog) abgearbeitet werden**.

...über aufeinander abgestimmte Notfallkonzepte zu verfügen. **Dabei muss gewährleistet sein, dass das Auslagerungsunternehmen die Wiederanlaufbedingungen (z.B. RTO) des auslagernden Instituts umsetzt.**

Im Notfallkonzept werden Verantwortlichkeiten, **zusätzlich erforderliche Kompetenzen,**…

...sowie für das Auslösen **und Deaktivieren** der Pläne definiert.

AT 7.3 Notfallkonzept – 3

Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig zu überprüfen. Für zeitkritische Aktivitäten und Prozesse ist sie für alle relevanten Szenarien mindestens jährlich und anlassbezogen nachzuweisen. Überprüfungen des Notfallkonzeptes sind zu protokollieren. Ergebnisse sind hinsichtlich

notwendiger Verbesserungen zu analysieren. Risiken sind angemessen zu steuern. Die Ergebnisse sind den jeweiligen Verantwortlichen schriftlich mitzuteilen.

Überprüfungen des Notfallkonzeptes
Die Häufigkeit und der Umfang der Überprüfungen soll sich grundsätzlich an der Gefährdungslage orientieren. Dienstleister sind angemessen einzubinden. Überprüfungen beinhalten u. a.:
- Test der technischen Vorsorgemaßnahmen
- Kommunikations-, Krisenstabs- und Alarmierungsübungen
- Ernstfall- oder Vollübungen.

Erläuterung, Hinweise und Fragen des IBCRM e.V.

Unseres Erachtens ist die jährliche Wirksamkeitsprüfung für ALLE relevanten Szenarien ihrem Zweck wenig förderlich. Die Forderung führt zu

- einer vermehrten Nutzung von theoretischen Übungen (Table Top Exercises) anstelle in ihrem Format angemessen gewählten Übungen und
- einer aufwandsbegründeten Reduktion von Ausfallszenarien – eine Relevanz-begründeten Menge an für die Notfallkonzeption zugrunde gelegten Szenarien ersetzend.

Diese Anforderung sollte über einen drei Jahreszyklus entzerrt werden.

Wir freuen uns über eine Berücksichtigung unserer Änderungs- und Ergänzungsvorschläge. Bei Fragen stehen wir Ihnen gern unter info@ibcrm.de zur Verfügung.

Mit freundlichen Grüßen

– Der Vorstand –

Institut für Business Continuity & Resilience Management e.V.

1. Vorstand: Franziska Hain
2. Vorstand: Sandra Achilles

Adresse Postfach 21 01 71
50527 Köln
Email info@ibcrm.de
Webseite www.ibcrm.de

Bank Kreissparkasse Köln (KSK)
BIC COKSDE33XXX
IBAN DE13 3705 0299 0012 008 003
VR-Nr. 19274 Amtsgericht Köln
Steuernummer 220 5992 1872