

Leitlinie Business Continuity Management (Dokumentvorlage)

Hilfsmittel zum BSI-Standard 200-4

Dokumenteigenschaften

|  |  |
| --- | --- |
| **Kennzeichnung** | **Erläuterung** |
| Titel: | *Leitlinie BCM* |
| Klassifikation (Einstufung): | Öffentlich | *Intern* | Vertraulich | Streng vertraulich |
| **Versionsnummer:** | *1.0* |
| **Zuständig:** | *Max Mustermann (BCM-Beauftragter)* |
| **Ablageort:** | *<Intranetlink>, Büro des BCM-Beauftragten* |
| **Zielgruppe:** | *Alle Mitarbeiter der Institution, berechtigte Interessengruppen (zur Einsichtnahme)* |
| **Erstellt am:** | *10.02.2021* |
| **Erstellt von:** | *Max Mustermann (BCM-Beauftragter)* |
| **Letzte Überarbeitung:** | *01.03.2021* |
| **Nächste Überarbeitung:** | *01.03.2021* |
| **Freigabe am:** | *15.03.2021* |
| **Freigabe durch:** | *Institutionsleitung* |

Tabelle : Dokumenteigenschaften

Änderungshistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Name | Beschreibung |
| 0.9 | *10.02.2021* | *Max Mustermann (BCM-Beauftragter)* | *Ersterstellung* |
| *1.0* | *01.03.2021* | *Institutionsleitung* | *Freigegebene, veröffentliche Version* |

Tabelle : Änderungshistorie

Musterinstitution

Muster-PLZ Musterstadt

Tel: +49 222 1111111111-0

E-Mail: mustermann@musterinstitution.de

Internet: https://www.musterinstitution.de

Inhalt

[1 Erläuterung der Dokumentvorlage 5](#_Toc73954769)

[2 Motivation und Zielsetzung 6](#_Toc73954770)

[3 Geltungsbereich 6](#_Toc73954771)

[4 Regulatorische und sonstige Anforderungen 7](#_Toc73954772)

[5 Definitionen 7](#_Toc73954773)

[6 Rollen, Aufgaben und Zuständigkeiten 7](#_Toc73954774)

[7 Kontrolle der Einhaltung 8](#_Toc73954775)

[8 Kontinuierliche Verbesserung 8](#_Toc73954776)

[9 Freigabe und Aktualisierung der Leitlinie 9](#_Toc73954777)

Erläuterung der Dokumentvorlage

*Die Leitlinie wird in der Regel durch den BCM-Beauftragten erstellt und fasst die Entscheidungen der Institutionsleitung zur Etablierung des BCMS zusammen. Zudem dokumentiert die Leitlinie die Selbstverpflichtung der Institutionsleitung, ein BCMS zu initiieren, betreiben und kontinuierlich weiterentwickeln zu lassen.*

*Diese Dokumentvorlage soll bei der Erstellung der Leitlinie unterstützen und beinhaltet alle relevanten Aspekte gemäß BSI-Standard 200-4 Kapitel 6.3 Leitlinie. Das Dokument beinhaltet in kursiver und blauer Schrift dargestellte Beispieltexte, die ausformuliert und institutionsspezifisch konkretisiert werden müssen. Die Beispiele reflektieren die jeweiligen Anforderungen des Standard-BCMS. Wird das Hilfsmittel für ein Reaktiv-BCMS genutzt, können die nicht relevanten Passagen gestrichen werden.*

*Dieser Abschnitt dient nur der Erläuterung der Dokumentvorlage und sollte nach Fertigstellung des Dokuments gelöscht werden.*

# Motivation und Zielsetzung

*Der Aufgabenzweck der <Institution> umfasst <Beschreibung der Hauptaufgabe>. Ein Ausfall des Geschäftsbetriebs hätte direkten Einfluss auf die Erfüllung ihres öffentlichen Auftrags/finanzielle Lage/Existenz der Institution, das Vertrauen der Bürger/Kunden sowie die öffentliche Ordnung/öffentliche Versorgungssicherheit.*

*Mit Hilfe des Business Continuity Managements (BCM) werden die zeitkritischen Geschäftsprozesse der <Institution> gegen ungeplante Unterbrechungen angemessen abgesichert.*

*Zeitkritisch sind Geschäftsprozesse, deren Ausfall innerhalb des Betrachtungszeitraums von <14 Tagen> zu einem nicht tolerierbaren Schaden für die <Institution> führen können. Als zeitkritisch gelten ebenfalls die Ressourcen, die zur Aufrechterhaltung dieser zeitkritischen Geschäftsprozesse benötigt werden. Der genannte Betrachtungszeitraum ergibt sich aus den gesetzlichen Anforderungen/den zu berücksichtigenden Risiken/den Erwartungen der Interessengruppen der <Institution>/etc.. Der Betrachtungszeitraum für das BCM wird als Planungsgrundlage für die Notfallvorsorge verwendet und legt den zeitlichen Rahmen fest, innerhalb dessen die zeitkritischen Geschäftsprozesse und Ressourcen der <Institution> mittels Notfallplänen und -maßnahmen abgesichert werden.*

*Das BCM ermöglicht es der <Institution> in einer Notfall- oder Krisensituation, die zeitkritischen Geschäftsprozesse auf einem vorab definierten Notbetrieb schnell wiederanlaufen und fortführen zu können und schnellstmöglich in den Normalbetrieb zurückzukehren.*

*Im Rahmen des BCM-Systems (BCMS) werden sowohl eine BCM-Organisation sowie BCM-Prozessschritte, Maßnahmen und Pläne zur Notfallvorsorge als auch zur Notfallbewältigung etabliert, gesteuert und überwacht.*

*Die <Institution> verfolgt damit die folgenden Ziele:*

* *Die Sicherstellung der Aufgabenerfüllung der <Institution> gegenüber <(nachgeordneten) Institutionen/Geschäftspartnern> sowie den <Bürgern/Kunden>.*
* *Die Sicherstellung, dass relevante Gesetze, Vorschriften, Normen und Standards eingehalten werden und Regressforderungen, Bußgelder, Strafen und Schadenersatz durch Anforderungen an das BCM angemessen verhindert werden.*
* *Den Schutz der Reputation der <Institution> in der Öffentlichkeit insbesondere bei Unterbrechungen des Geschäftsbetriebs.*

*Das BCM der <Institution> orientiert sich methodisch am BSI-Standard 200-4 „Business Continuity Management“.*

# Geltungsbereich

*Das BCMS der <Institution> umfasst alle Standorte, Organisationseinheiten und Geschäftsprozesse der <Institution>.*

*Die Leitlinie und sich daraus ableitenden Anforderungen zum BCM gelten sowohl für interne und externe Mitarbeiter und ist auch für die Einbindung von Dienstleistern bindend, sofern diese zeitkritischen Dienste oder Leistungen für <die Institution> erbringen oder in zeitkritische Geschäftsprozesse eingebunden sind.*

# Regulatorische und sonstige Anforderungen

*Die für die Institution maßgeblichen regulatorischen Anforderungen zum BCM umfassen:*

* *<Umsetzungsplan Bund (UP BUND)>*
* *<IT-Sicherheitsgesetz>*
* *<Vertragliche Anforderungen der Institution/des Geschäftspartners XYZ>*
* *[…]*

*Des Weiteren sind die Bedürfnisse und Erwartungen der Interessengruppen an einen kontinuierlichen Geschäftsbetrieb maßgeblich für die Ausgestaltung des BCM der <Institution>. Hierbei werden die internen Interessengruppen (d.h. Führungskräfte, Mitarbeiter, Informationssicherheitsbeauftragter, BCM-Rolleninhaber, Revision, […]) und externen Interessengruppen (d.h. Bürger, <(nachrangige) Institutionen>, <Dienstleister>, […]) <jährlich> und anlassbezogen betrachtet.*

# Definitionen

***Störung***

*Eine Störung ist eine Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen. Störungen werden in der Regel innerhalb des Normalbetriebs durch die Allgemeine Aufbauorganisation der Institution behoben. Hierzu wird auf vorhandene Prozesse zur Störungsbeseitigung oder des Incident-Managements zurückgegriffen. Störungen können jedoch zu einem Notfall eskalieren.*

***Notfall***

*Notfälle sind Unterbrechungen des Geschäftsbetriebs, die mindestens einen zeitkritischen Geschäftsprozess betreffen, der nicht im Normalbetrieb innerhalb der maximal tolerierbaren Ausfallzeit wiederhergestellt werden kann. Im Gegensatz zu Störungen wird zur Bewältigung von Notfällen eine BAO benötigt. Im Gegensatz zur Krise liegen hier geeignete Pläne zur Bewältigung vor oder bestehende Pläne können adaptiert werden. Notfälle können auch eintreten, bevor das Schadensereignis zu einer Unterbrechung des Geschäftsbetriebs führt. Es genügt die Gefahr, dass durch das Schadensereignis der Geschäftsbetrieb unterbrochen wird.*

***Krise***

*Als Krise wird ein Schadensereignis bezeichnet, das sich in massiver Weise negativ auf die Institution auswirkt und dessen Auswirkungen auf die Institution nicht im Normalbetrieb bewältigt werden können. Im Gegensatz zu einem Notfall liegen zur Bewältigung einer Krise jedoch keine spezifischen Notfallpläne vor, vorhandene Notfallpläne können nicht oder nur bedingt adaptiert werden oder greifen schlicht nicht. Innerhalb der Institution wird die Krise durch eingeleitete Maßnahmen der BAO bewältigt. Krisen können unmittelbar auftreten oder aus einer Störung oder einem Notfall heraus eskalieren.*

# Rollen, Aufgaben und Zuständigkeiten

*Die BCM-Organisation besteht aus den folgenden Rollen:*

*Die* ***Institutionsleitung*** *verantwortet den BCM-Prozess. Sie legt die Bedeutung und Ziele des BCM in der Institution fest, bestimmt dessen Geltungsbereich und stellt die notwendigen finanziellen und personellen Ressourcen zur Verfügung. Für die weitere Ausgestaltung und die Umsetzung des BCMS ernennt die Institutionsleitung einen BCM-Beauftragten. Die Institutionsleitung fordert aktiv Informationen über den Status Quo des BCM ein und steuert die Weiterentwicklung des BCM durch ihre Entscheidungen.*

*Der* ***BCM-Beauftragte*** *(BCMB) steuert alle Aktivitäten rund um die Notfallvorsorge und wirkt bei den damit verbundenen Aufgaben mit. Er ist dafür zuständig das BCMS sowie die zugehörigen Prozesse, Methoden, Verfahren und Rollen in Abstimmung mit der Institutionsleitung zu definieren, zu implementieren und weiterzuentwickeln. Ferner ist der BCM-Beauftragte dafür zuständig die Vorgaben im BCM zu überwachen und der Institutionsleitung zyklisch Bericht über den Zustand des BCMS zu erstatten. Der BCM-Beauftragte wird hierzu von der Institutionsleitung mit den erforderlichen Rechten ausgestattet.*

*Ferner kann der BCMB weitere erforderliche Rollen der BCM-Organisation und deren Zuständigkeiten im Normalbetrieb sowie im Notfall gemeinsam mit der Institutionsleitung definieren.*

*In allen nachfolgenden Dokumenten zum BCM wird zwecks besserer Abgrenzung zwischen der allgemeinen Aufbauorganisation (BCM-AAO) und der Besonderen Aufbauorganisation (BCM-BAO) unterschieden.*

* *Die BCM-AAO umfasst alle Rollen, die in der Notfallvorsorge aktiv sind oder das BCMS betreiben und kontinuierlich weiterentwickeln.*
* *Die BCM-BAO umfasst alle Rollen, die zum Zweck einer effektiven und schnellen Notfallbewältigung vom Normalbetrieb abweichende Aufgaben und Zuständigkeiten innehaben.*

*Unabhängig von der definierten BCM-Organisation stellen* ***alle Mitarbeiter*** *einen wichtigen Bestandteil des BCM dar, um die Institution gegenüber Schadensereignissen und deren Auswirkungen resilienter zu machen. Daher sind alle Mitarbeiter aufgefordert, in ihren jeweiligen Aufgabenbereichen die BCM-Organisation darin zu unterstützen, das BCMS zu etablieren, aufzubauen und kontinuierlich weiterzuentwickeln.*

# Kontrolle der Einhaltung

*Die Vorgaben dieser Leitlinie und nachrangiger Dokumente im BCM werden vom BCM-Beauftragten regelmäßig sowie anlassbezogen auf Einhaltung kontrolliert. Der BCM-Beauftragte kann in Abstimmung mit der Institutionsleitung auch externe Stellen mit Überprüfungen beauftragen.*

*Um erforderliche Korrekturmaßnahmen umsetzen zu lassen, verfügt der BCM-Beauftragte über ein fachliches Weisungsrecht gegenüber den BCM-Rolleninhabern der BCM-Vorsorgeorganisation.*

*Die interne Revision hat den aufsichtsrechtlichen Auftrag, risikoorientiert und unabhängig die Wirksamkeit und Angemessenheit des BCMS sowie die Ordnungsmäßigkeit grundsätzlich aller Aktivitäten und Prozesse <jährlich> zu prüfen.*

# Kontinuierliche Verbesserung

*Der BCM-Beauftragte überprüft kontinuierlich das BCMS dahingehend, ob dieses gemäß den Zielen und Anforderungen des BCM aktuell, angemessen, effektiv und effizient ist. Der BCM-Beauftragte identifiziert Abweichungen vom vorgegebenen Managementsystem und leitet erforderliche Korrektur- und Verbesserungsmaßnahmen ein. Er kontrolliert, ob die Maßnahmen rechtzeitig umgesetzt wurden und ob die umgesetzten Maßnahmen die Abweichungen hinreichend sowie nachhaltig beseitigt wurden und zur gewünschten Verbesserung führen.*

# Freigabe und Aktualisierung der Leitlinie

*Die Institutionsleitung gibt die vorliegende Leitlinie frei und übernimmt damit die Verantwortung für das BCM.*

*Der BCM-Beauftragte überprüft jährlich die Leitlinie auf Änderungsbedarf. Die Leitlinie muss bei wesentlichen Änderungen der Rahmenbedingungen oder Ziele des BCM angepasst und erneut durch die Institutionsleitung freigegeben werden.*

*Die Leitlinie wird nach erstmaliger Freigabe oder Aktualisierung allen internen Interessengruppen via Intranet/… bekanntgegeben und relevanten externen Interessengruppen auf Nachfrage zur Verfügung gestellt.*

*<Ort, Datum>*

*<Institutionsleitung> <Institutionsleitung> <Institutionsleitung> BCM-Beauftragter*