

Grundanforderungskatalog BCM (Dokumentvorlage)

Hilfsmittel zum BSI-Standard 200-4

Dokumenteigenschaften

|  |  |
| --- | --- |
| **Kennzeichnung** | **Erläuterung** |
| **Titel** | *Grundanforderungskatalog BCM* |
| **Klassifikation (Einstufung):** | *Öffentlich | ~~Intern~~ | ~~Vertraulich~~ | ~~Streng vertraulich~~* |
| **Versionsnummer:** | *1.0* |
| **Zuständig:** | *Max Mustermann (BCM-Beauftragter)* |
| **Ablageort:** | *<Intranetlink>* |
| **Zielgruppe / Verteiler:** | *Alle BAO-Rollen und Auftragnehmer* |
| **Erstellt am:** | *10.05.2021* |
| **Erstellt von:** | *Max Mustermann (BCM-Beauftragter)* |
| **Letzte Überarbeitung:** | *01.06.2021* |
| **Nächste Überarbeitung:** | *01.06.2022* |
| **Freigabe am:** | *15.05.2021* |
| **Freigabe durch:** | *Institutionsleitung* |

Tabelle : Dokumenteigenschaften

Änderungshistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Name | Beschreibung |
| *0.9* | *10.05.2021* | *Max Mustermann (BCM-Beauftragter)* | *Ersterstellung* |
| *1.0* | *01.06.2021* | *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

[*Erläuterung der Dokumentvorlage* 5](#_Toc77161324)

[1 Einleitung 6](#_Toc77161325)

[2 Grundanforderungskatalog 7](#_Toc77161326)

# *Erläuterung der Dokumentvorlage*

*Das vorliegende Hilfsmittel unterstützt dabei, den Grundanforderungskatalog aus Kapitel 7 BCM im Rahmen des Outsourcings und von Lieferketten des BSI-Standard 200-4 institutionsspezifisch zu erstellen. Das Hilfsmittel beinhaltet in kursiver und blauer Schrift dargestellte Beispieltexte, die institutionsspezifisch konkretisiert und ausformuliert werden müssen. Insbesondere die verwendeten Modalverben (muss, sollte) müssen auf den individuellen Bedarf und die Risikosituation der Institution angepasst werden.*

*Die in den Beispielen genannten „relevanten“ Aspekte beziehen sich jeweils auf den zeitkritischen Leistungsbezug. So muss beispielsweise der Dienstleister nicht für alle seine zeitkritischen Geschäftsprozesse und Ressourcen BC-Pläne vorweisen, sondern nur die für den zeitkritischen Leistungsbezug relevanten. Ferner richtet sich die Angemessenheit der Maßnahmen des Dienstleisters an den Vorgaben der Institution aus. So ist die Formulierung „angemessen und regelmäßig geübt und getestet“ beispielsweise so zu verstehen, dass der Dienstleister Übungsarten anwendet, die auch die Institution für den zeitkritischen Leistungsbezug vorsehen würde und die Übungshäufigkeit sowie Übungskomplexität auf einem Niveau sichergestellt ist, das dem der Institution entspricht. Wird dies aus den Beispielen übernommen, sollte auch dieser Text sinngemäß übernommen werden.*

# Einleitung

*Sofern eine Institution zeitkritische Leistungen von externen Dienstleistern bezieht, sollte der BCMB laut BSI-Standard 200-4, Kapitel 7 BCM im Rahmen des Outsourcings und von Lieferketten BCM-Grundanforderungen definieren, die bei der Dienstleisterauswahl berücksichtigt werden sollten. Hierzu sollte ein Grundanforderungskatalog erstellt werden.*

*Unabhängig von den konkreten SLAs, die für den Notfall auch vom Dienstleister erfüllt werden müssen, dient der Grundanforderungskatalog dazu, Anforderungen zu listen, die sicherstellen sollen, dass der Dienstleister prinzipiell in der Lage ist, angemessen auf Notfälle zu reagieren. Mit dem Grundanforderungskatalog soll die folgende Frage untersucht werden: Hat der Dienstleister prinzipiell ausreichende Strukturen etabliert, um im Notfall irgendwie geartete SLAs sicherzustellen? Dieser Nachweis könnte über ein zertifiziertes BCMS oder über ein Dritt-Audit z. B. aus einem Audit-Pool leicht erbracht werden. Jedoch verfügt nicht jeder Dienstleister über solche Nachweise oder diese decken nicht (vollständig) den zeitkritischen Leistungsbezug ab. Daher kann es sinnvoll sein, im Anforderungskatalog nicht einfach die Zertifizierung oder ein Dritt-Audit zu fordern, sondern die Anforderungen an die Strukturen beim Dienstleister <gegebenenfalls nach Zeitkritikalität abgestuft> separat aufzulisten. Die in diesem Grundanforderungskatalog gelisteten Anforderungen sollten bei der Auswahl von Dienstleistern immer berücksichtigt werden.* *Der Grundanforderungskatalog kann auch als Baukasten für verschiedene Outsourcing Kategorien eingesetzt werden.*

# Grundanforderungskatalog

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Thema** | **Anforderungsinhalt** | **Mögliche Evidenzen** |
| *BCM-GA-01* | *BCM-Aufbauorganisation* | * *Die BCM-Aufbauorganisation muss festgelegt sein.* * *Die Aufgaben, Zuständigkeiten und erforderliche Fähigkeiten und Kenntnisse müssen schriftlich belegt sein.* * *Die festgelegten Rollen müssen durch qualifizierte Mitarbeiter besetzt sein.* | * *Rollen-/Stellenbeschreibung(en)* * *Ernennungsurkunde(n)* * *Schulungsnachweise* |
| *BCM- GA-02* | *Schulung / Sensibilisierung* | * *BCM-Rolleninhaber müssen regelmäßig und bedarfsgerecht geschult werden.* * *Ein Schulungs- und Sensibilisierungskonzept für das Thema BCM sollte vorhanden sein.* | * *Schulungs- und Sensibilisierungskonzept* * *Teilnahme-Nachweise* |
| *BCM- GA-03* | *Business Impact Analyse* | * *Zeitkritische Geschäftsprozesse und Ressourcen müssen regelmäßig mittels einer Business Impact Analyse (BIA) identifiziert und analysiert werden.* | * *Dokumentierter Nachweis zur Vorgehensweise und Methodik* * *BIA-Ergebnisse* |
| *BCM- GA-04* | *BCM-Risikoanalyse* | * *Relevante Risiken für zeitkritische Geschäftsprozesse und Ressourcen sollten regelmäßig identifiziert und analysiert werden.* * *Identifizierte Risiken müssen angemessenen behandelt werden.* | * *Dokumentierter Nachweis zur Vorgehensweise und Methodik* * *Ergebnisse der Risikoanalyse* |
| *BCM- GA-05* | *Business Continuity Strategien und  -Lösungen* | * *Es müssen Business Continuity Strategien definiert sein, die verschiedene relevante Ausfallszenarien abdecken (z. B. Gebäudeausfall, IT-Ausfall, Personalausfall).* * *Die Business Continuity Strategien und -Lösungen sollten die Ergebnisse der BIA und identifizierte BCM-Risiken berücksichtigen.* * *Die Business Continuity Strategien und -Lösungen sollten regelmäßig überprüft werden* | * *Dokumentierte Business Continuity Strategien und –Lösungen* * *Begehung(en)* |
| *BCM- GA-06* | *Aufbau und Befähigung einer besonderen Aufbauorganisation* | * *Eine besondere Aufbauorganisation (BAO) sowie deren Arbeitsweise zur zielgerichteten und raschen Bewältigung eines Ereignisses müssen definiert und etabliert sein.* * *Es muss definiert und dokumentiert sein, wie Ereignisse zeitgerecht eskaliert und die zuständigen Rollen alarmiert werden.* * *Es sollten Sofortmaßnahmen definiert sein, die unmittelbar nach Eintritt eines Schadensereignisses eingeleitet werden können, um weitere Schäden abzuwenden.* * *Es müssen Regelungen zur Notfallkommunikation definiert und dokumentiert sein, mit der eine zeitnahe Information an den Auftraggeber ermöglicht wird.* | * *Notfallhandbuch / Dokumentation zur Notfallbewältigung / Geschäftsordnung des Stabs* * *ggf. vorhandene Sonderpläne (etwa Sofortmaßnahmenplan, Alarmierungs- und Eskalationsplan, Notfallkommunikationsplan)* |
| *BCM- GA-07* | *Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungspläne* | * *Es müssen Pläne dokumentiert sein, mit denen die relevanten, zeitkritischen Geschäftsprozesse zeitgerecht fortgeführt werden können.* * *Es müssen Pläne dokumentiert sein, mit denen die relevanten, zeitkritischen Ressourcen wiederanlaufen und wiederhergestellt werden können.* | * *Dokumentierte Notfallpläne (z. B. Geschäftsfortführungspläne, Wiederanlaufpläne, Wiederherstellungspläne)* |
| *BCM- GA-08* | *Üben und Testen* | * *Es sollte eine Übungsplanung vorhanden sein.* * *Alle relevanten BC-Pläne und BC-Maßnahmen müssen angemessen und regelmäßig geübt und getestet werden.* | * *Übungshandbuch* * *Jahresübungsplan* * *Übungskonzepte* * *Übungsprotokolle* * *Übungsberichte* |
| *BCM- GA-09* | *Leistungsüberprüfung und Berichterstattung* | * *Es muss regelmäßig überprüft werden, ob das BCMS angemessen, wirksam und effizient ist beziehungsweise ob Korrekturbedarfe oder Verbesserungsmöglichkeiten bestehen.* * *Zur Leistungsüberprüfung sollten Kennzahlen erhoben und ausgewertet werden* * *Zur Wirksamkeitsüberprüfung sollten interne und externe Überprüfungen durchgeführt werden.* * *Die Leitungsebene der Institution sollte ihre Aufgabe als Gesamtverantwortliche des BCMS wahrnehmen und regelmäßig den aktuellen Status des BCM überprüfen, bewerten und erforderlichenfalls korrigieren.* | * *Leitlinie* * *Prüfprogramm* * *Prüfberichte* * *Beschlüsse aus Sitzungen der Leitungsebene* * *Management Reviews* |
| *BCM- GA-10* | *Korrektur und Verbesserung des BCMS* | * *Identifizierte Korrekturbedarfe und Verbesserungsmöglichkeiten müssen durch Maßnahmen behandelt.* * *Die Wirksamkeit der umgesetzten Korrekturmaßnahmen muss kontrolliert werden.* | * *Maßnahmenplan* |
| *BCM- GA-11* | *Dienstleistersteuerung* | * *Zeitkritische (Sub-)Dienstleister müssen identifiziert werden* * *Mit relevanten, zeitkritischen (Sub-)Dienstleistern müssen angemessene BCM-Vertragsanforderungen vereinbart werden.* | * *Vertragsformulierungen mit BCM-Bezug* |
| *…* |  |  |  |