DZ BANK

ANFORDERUNGEN AN DAS BCM DES AUFTRAGNEHMERS

1. VERANTWORTUNG DER GESCHÄFTSFÜHRUNGSEBENE

1.1. Die Geschäftsführungsebene hat die Gesamtverantwortung für das Business Continuity Management (BCM) zu tragen sowie die Ziele und den Geltungsbereich verbindlich und nachvollziehbar festzulegen und zu dokumentieren. Zudem muss der Prozess für das BCM initiiert, gesteuert und kontrolliert werden.

1.2. Die Geschäftsführungsebene hat dafür Sorge zu tragen, dass das BCM-System regelmäßig auf Aktualität und Angemessenheit überprüft und bewertet wird und bei Bedarf korrigierende Maßnahmen eingeleitet werden. Wenn die operative Ausführung dieser Aufgaben durch die Geschäftsführung delegiert wird, ist dies durch eine zentrale Rolle (z.B. Business Continuity Manager) umzusetzen.

1.3. Die Geschäftsführungsebene hat sich bzw. ist regelmäßig, mindestens jedoch jährlich, über den Stand des BCM, z.B. durch Statusberichte BCM-Aktivitäten und -Ergebnisse, Risiken) zu informieren.

1.4. Die Geschäftsführungsebene hat sicherzustellen, dass ausreichend finanzielle, technische und personelle Ressourcen für die angestrebten Ziele des BCM bereitgestellt werden und die Ressourcen jährlich sowie anlassbezogen auf die aktuellen Anforderungen hin zu überprüfen und ggf. anzupassen sind.

2. ANFORDERUNGEN, GELTUNGSBEREICH UND ZIELE

2.1. Die mit der DZ BANK vereinbarte Leistung muss im Geltungsbereich (Scope) des BCM-Systems liegen.

2.2. Die methodische Ausrichtung des Vorgehensmodells zur Etablierung und zum kontinuierlichen Betrieb des BCM ist innerhalb einer Leitlinie zu beschreiben (z. B. Orientierung an BSI-Standard zum BCM oder ISO 22301). Die Leitlinie ist sowohl in regelmäßigen Abständen (mindestens alle 4 Jahre) als auch bei wesentlichen Änderungen der Rahmenbedingungen, Geschäftsziele, Aufgaben oder Strategien auf ihren Anpassungsbedarf zu überprüfen und bedarfsweise zu aktualisieren.

3. AUFGABEN, KOMPETENZEN UND VERANTWORTLICHKEITEN

3.1. Die Rollen des BCM sowie die jeweiligen Aufgaben, Pflichten und Kompetenzen dieser Rollen sind gemäß den Gegebenheiten angemessen festzulegen und zu dokumentieren. Dies beinhaltet die formale Ernennung eines für die Aufrechterhaltung und Weiterentwicklung des BCM zuständigen Notfallmanagers/ -beauftragten bzw. Business Continuity Managers.

3.2. Die Organisationsstruktur im BCM ist jährlich auf ihre Angemessenheit hin zu überprüfen. Veränderungen sind zu berücksichtigen (z.B. Veränderungen hinsichtlich Größe, zu berücksichtigende Standorte oder Organisationseinheiten

4. SCHNITTSTELLEN, GREMIEN UND KOMMUNIKATION

4.1. Alle Vorgaben, Prozesse und Verantwortlichkeiten im BCM sind regelmäßig und anlassbezogen mit korrespondierenden Managementdisziplinen, die der Sicherstellung und Einhaltung von Schutzzielen dienen, abzustimmen und im Sinne einer Gesamtsicherheitsstrategie aufeinander auszurichten.

5. SCHULUNG UND SENSIBILISIERUNG

5.1. Mitarbeiter mit Aufgaben und Verantwortlichkeiten im BCM sind entsprechend ihrer benötigten Kompetenz zu schulen sowie jährlich über ihre rollenspezifischen Aufgaben und Veränderungen im BCM zu informieren.

5.2. Alle Mitarbeiter sind regelmäßig (min. alle 2 Jahre) für das Thema BCM zu sensibilisieren.

5.3. Maßnahmen zur Schulung und Sensibilisierung sind in einem Schulungs- und Sensibilisierungsprogramm zum BCM zu dokumentieren, sowie die durchgeführten Maßnahmen zu dokumentieren (z.B. durch Teilnehmerlisten, Zertifikate, Teilnahmebescheinigungen).

6. BUSINESS IMPACT ANALYSE (BIA) – METHODIK

6.1. Jährlich sowie anlassbezogen ist eine systematische Analyse der Auswirkungen eines Ausfalls aller Geschäftsprozesse/ Aktivitäten bzw. Aktivitäten pro Organisationseinheit durchzuführen (Business Impact Analyse). Diese Analyse muss einen Zeitbezug haben (z.B. erwartete Schäden durch einen Ausfall von Geschäftsprozessen/Aktivitäten innerhalb der Kategorien <4 Stunden, <1 Tag… <5 Tage). Bereits vorhandene Ergebnisse (z.B. BIA-Ergebnisse aus dem Vorjahr) können als Grundlagen herangezogen werden und sind entsprechend zu aktualisieren.

6.2. Bei der Schadensbewertung müssen neben wirtschaftlichen/ finanziellen Auswirkungen auch mögliche Reputationsverluste und rechtliche Auswirkungen berücksichtigt werden.

6.3. Im Rahmen der durchzuführenden BIA müssen mindestens die Ressourcen: Gebäude, Personal, IT und Dienstleister betrachtet werden.

6.4. Die Analyse der Auswirkungen eines Ausfalls von Geschäftsprozessen/ Aktivitäten muss folgende Informationen ermitteln:

- Maximal tolerierbare Ausfallzeit (MTPD)
- Geplante Wiederanlaufzeit in einem Notbetrieb (RTO)

6.5. Abhängigkeiten der Geschäftsprozesse/ Aktivitäten untereinander (Prozessketten) sowie die für einen Notbetrieb erforderlichen, d.h. zeitkritische Ressourcen (insbesondere Arbeitsplätze, IT, personelle Rollen/ Funktionen, Auslagerungen und Fremdbezüge) müssen erhoben, dokumentiert und bei Abhängigkeiten untereinander vererbt werden.

6.6. Die Methodik und das Vorgehen zur Business Impact Analyse ist anhand einer Methoden- und Prozessbeschreibung nachvollziehbar zu dokumentieren.

6.7. Für Geschäftsprozesse/ Aktivitäten, die zur Bewältigung von IT- oder IT-Sicherheit-bezogenen Notfällen und Krisen unabdingbar sind, ist sicherzustellen, dass diese in die höchste Verfügbarkeitsanforderung eingestuft werden.

7. RISIKOANALYSE

7.1. Jährlich sowie anlassbezogen ist eine systematische Einschätzung potenzieller Risiken, die zu einem Ausfall von Geschäftsprozessen/ Aktivitäten bzw. Ressourcen führen können, durchzuführen. Die Methodik zur Durchführung der RA ist zu dokumentieren. Neue Risiken sind gemäß o.g. Methodik zu analysieren; bereits identifizierte und bewertete Risiken sind auf Veränderung zu prüfen. Bereits vorhandene Ergebnisse (z.B. RA-Ergebnisse aus dem Vorjahr) können als Grundlagen herangezogen werden und sind entsprechend zu aktualisieren.

7.2. Die Risikoanalyse ist so konzipiert, dass ein Katalog von Risiken und Szenarien betrachtet wird, welcher auf gängigen Standards und aktuell gültigen aufsichtsrechtlichen Anforderungen basiert.

7.3. Die Ergebnisse der Risikoanalyse sind zu dokumentieren und der Geschäftsführungsebene zur Kenntnisnahme zur Verfügung zu stellen (ggf. im Rahmen eines Gesamtrisikostatus).

8. NOTFALLSTRATEGIEN UND RISIKOBEHANDLUNG

8.1. Auf Basis der Ergebnisse der Business Impact Analyse und Risikoanalyse sind angemessene Notfallstrategien zu entwickeln und zu aktualisieren, die einen Wiederanlauf der kritischen Geschäftsprozesse/ Aktivitäten in den Notbetrieb innerhalb der geforderten Zeit, eine Aufrechterhaltung des Notbetriebs sowie eine Wiederherstellung und Rückführung in den Normalbetrieb ermöglichen.

8.2. Mindestens für die zeitkritischen Ressourcen ist für jedes identifizierte Risiko, das gemäß der Risikoanalyse einen Handlungsbedarf zur Risikobehandlung umfasst und für die keine dokumentierte Risikoübernahme vorliegt, ein Risikobehandlungsplan zur Reduzierung der Auswirkungen, Eintrittswahrscheinlichkeit oder Ausfallzeit zu entwickeln.

8.3. Eine abschließende Risikoübernahme des Restrisikos ist vom Risikoeigner durchzuführen und zu dokumentieren.

9. NOTFALLDOKUMENTATION

9.1. Es sind Dokumentationen (BC-Plan/Notfallplan) zu entwickeln, die bei einer signifikanten Unterbrechung des Geschäftsbetriebs aktiviert werden und in denen die notwendigen Aktivitäten beschrieben sind, wie ein definierter Notbetrieb, basierend auf den Verfügbarkeitsanforderungen der Business Impact Analyse, erreicht und aufrechterhalten werden kann.

9.2. Die Dokumentation (BC-Plan/Notfallplan) muss die Vorbereitung des Notfallbetriebs sowie die Rückführung aus dem Notbetrieb für die Szenarien Personalausfall (z.B. durch Ausfall von Schlüsselpersonal, Pandemie), Gebäudeausfall (z.B. durch Naturkatastrophen, Stromausfall), IT-Ausfall (z.B. durch Cyberangriff, substanzielle Fehler von IT-Assets oder der Kommunikationsinfrastruktur) und Dienstleisterausfall (z.B. durch Schlechtleistung, Streik) enthalten.

9.3. Es ist sicherzustellen, dass jährlich sowie anlassbezogen eine Vollständigkeits- bzw. Aktualisierungsprüfung aller reaktiven Notfalldokumente erfolgt.

10. IT-WIEDERANLAUF- UND WIEDERHERSTELLUNGSPLANUNG

10.1. Es ist sicherzustellen, dass für alle notfallrelevanten IT-Assets eine dokumentierte IT-Wiederanlaufplanung und IT-Wiederherstellungsplanung vorhanden ist, die den IT-Wiederanlauf der Ressource innerhalb der in der BIA ermittelten geforderten IT-Wiederanlaufzeit (RTO) sicherstellt.

10.2. Jährlich ist ein Abgleich der BIA-Ergebnisse mit dem letzten Stand der IT-Wiederanlaufplanung vorzunehmen (Soll-Ist-Vergleich zwischen RTO/ RPO aus BIA und Umsetzungsstatus). Bei Abweichungen ist sicherzustellen, dass Verbesserungsmaßnahmen eingeleitet werden.

10.3. Innerhalb der IT-Wiederanlaufplanung ist zu dokumentieren, in welcher Reihenfolge IT-Assets wiederaufgenommen werden, inklusive der voraussichtlichen Dauer des gesamten Wiederanlaufs.

11. BAULICHE/ TECHNISCHE RECHENZENTRUM-SICHERHEIT

11.1. Für alle Rechenzentren, in denen notfallrelevante IT-Assets betrieben werden, ist eine Gefährdungs- und Risikoanalyse zu erstellen, aus der hervorgeht, welche Schwachstellen und Bedrohungen am jeweiligen Standort zu erwarten sind. Hierbei sind insbesondere Umgebungsrisiken (wie z.B. Hochwasser, Erdbeben, etc.) und potenzielle Nachbarschaftsrisiken zu überprüfen.

11.2. Die Distanz der Rechenzentren zueinander ist hinsichtlich der Einhaltung gesetzlicher/ regulatorischer bzw. interner Vorgaben zu überprüfen und sicherzustellen. Die jeweilige Gefährdungs- und Risikosituation ist hierbei zu berücksichtigen.

12. DATENSICHERUNGEN

12.1. Es ist sicherzustellen, dass ein dokumentiertes Datensicherungskonzept vorhanden ist, welches den maximal tolerierbaren Datenverlust (RPO) aller notfallrelevanten IT-Assets und die damit verbundenen Daten regelt. Die Vorgaben sind auch für Offsite Storage anzuwenden.

12.2. Datensicherungsträger sind räumlich getrennt von den IT-Systemen zu lagern, auf denen die Daten gespeichert sind.

12.3. Es ist sicherzustellen, dass Datensicherungsträger redundant an einem entfernten Standort (mindestens separater Brandabschnitt) gelagert werden. Die Angemessenheit der Entfernung ist unter Berücksichtigung der individuellen Risiko- und Datensicherungssituation zu ermitteln.

12.4. Es ist sicherzustellen, dass ein ausreichend schneller Zugriff auf die Datensicherungen im Bedarfsfall gewährleistet ist.

12.5. Es sind jährliche Lesbarkeitstests von Datensicherungen durchzuführen. Die Ergebnisse sind zu protokollieren.

13. NOTFALL- UND KRISENORGANISATION

13.1. Es ist sicherzustellen, dass eine zentrale Steuerung, Koordinierung und Überwachung aller Aktivitäten in der Notfall- und Krisenbewältigung erfolgt und Verantwortlichkeiten für die Entscheidungsfindung auf strategischer Ebene in einem Not- und Krisenfall definiert und dokumentiert sind (z.B. durch einen Notfallstab oder Krisenstab).

13.2. Es ist sicherzustellen, dass durch organisatorische Regelungen ein geplantes und organisiertes Vorgehen innerhalb der Notfall- und Krisenbewältigung sichergestellt ist und die Anforderungen des Geschäftsbetriebs (speziell Verfügbarkeitsanforderungen gemäß Business Impact Analyse) berücksichtigt sind.

14. MELDUNG, ALARMIERUNG UND ESKALATION

14.1. Es sind Regelungen zur Meldung, Alarmierung und Eskalation von Schadensereignissen zu etablieren und dokumentieren, die folgende Aspekte abdecken:

- Festlegung von Schwellwerten (Grenze Störung/ Notfall),
- Qualifizierung des Ereignisses (Definition der Meldestellen, Entscheidung bzgl. der Qualifizierung eines Vorfalls als Notfall oder Krise),
- Aktivierung der reaktiven Notfall- und Krisenorganisation und
- zu nutzende Kommunikationswege.

15. NOTFALL-ÜBUNGEN/-TESTS

15.1. Die Planung von Übungen/ Tests sind in einem Übungs-/ Testprogramm (bspw. Jahresplan) zu dokumentieren. Dabei ist zu berücksichtigen: In einem Zeitraum von max. drei Jahren sind alle notfallrelevanten und als zeitkritisch eingestuften Geschäftsprozesse/Aktivitäten sowie alle zeitkritischen Ressourcen im Rahmen von Übungen/Tests zu berücksichtigen. Für Notfalltests bezogen auf IT-Assets müssen die Infrastruktur sowie die Komponenten eines Applikationsclusters berücksichtigt werden.

15.2. Bei der Planung des Übungs- und Testprogramms sind mindestens die Szenarien zu berücksichtigen, welche gemäß Eintrittswahrscheinlichkeit anhand der Gefährdungslage oder Risikoanalyse zu schwerwiegenden Not- oder Krisenfällen führen können.

15.3. Für zeitkritische IT-Assets (Verfügbarkeitsanforderung z.B. <4 Stunden oder <1 Tag) ist eine jährliche Durchführung von Wiederanlauftests verpflichtend durchzuführen. Für hoch zeitkritische IT-Assets (Verfügbarkeitsanforderung z.B. <4 Stunden) sind darüber hinaus alle 3 Jahre Wiederherstellungstests, bestehend aus einer System- und Datenwiederherstellung, durchzuführen.

15.4. Alle Übungs-/ Testergebnisse sind zu protokollieren.

15.5. Abgebrochene oder abgesagte Übungen/ Tests sowie Übungen/ Tests mit schwerwiegenden Feststellungen sind zu wiederholen bzw. neu zu planen. Dies ist im Übungs-/ Testprogramm entsprechend zu dokumentieren.

15.6. Alle Übungen/ Tests sind im Rahmen des Review-Prozesses (beachte Kapitel Reporting und Review) auf mögliche Folgemaßnahmen zu untersuchen.

15.7. In einem Zeitraum von max. drei Jahren ist eine Notfall-/ Krisenstabsübung unter Einbeziehung der Rollen/ Funktionen der Notfall-/ Krisenstabsorganisation durchzuführen.

16. AUSLAGERUNGEN UND FREMDBEZUG

16.1. Es ist sicherzustellen, dass die vereinbarten vertraglichen Regelungen (SLA) zwischen der DZ BANK und dem Dienstleister nicht durch die Weiterverlagerung an den Dritte negativ beeinträchtigt werden.

16.2. Extern betriebene notfallrelevante Dienstleistungen (weiterverlagerte Leistungen) müssen den SLA der DZ BANK (z.B. <4 Stunden für hoch zeitkritische Leistungen oder <1 Tag für zeitkritische Leistungen) entsprechen.

16.3. Für alle notfallrelevanten Auslagerungen und Fremdbezüge gilt es abgestimmte Notfallkonzepte zu entwickeln und diese jährlich auf Aktualität geprüft werden.

16.4. Externe Dienstleister sind dazu zu verpflichtet Kundenreports z.B.im Rahmen von ISAE3402- oder PS951-Reports zur Verfügung zu stellen, um die Einhaltung der Vorgaben bei Weiterverlagerungen zu dokumentieren.

17. KONTROLLHANDLUNGEN UND MAßNAHMEN-TRACKING

17.1. Die für das BCM verantwortlichen Rollen haben durch Definition und Durchführung systematischer Kontrollhandlungen sicherzustellen, dass die Methoden und Vorgaben zum BCM eingehalten werden.

17.2. Die Kontrollhandlungen und ihre jeweiligen Kontrollkriterien sind auf Grundlage der definierten Prozesse im BCM festzulegen und nachvollziehbar zu dokumentieren. Ebenfalls sind die Ergebnisse der Kontrollhandlungen zu dokumentieren und nachvollziehbar aufzubewahren.

17.3. Es ist sicherzustellen, dass Erkenntnisse aus eingetretenen Notfällen zu einer Prüfung und ggf. Anpassung der bestehenden Maßnahmen sowie organisatorischen und technischen Notfalldokumenten führen.

17.4. Die bei einer Überprüfung erkannten Probleme sind schnellstmöglich abzustellen. Die erforderlichen Korrekturmaßnahmen sind durch Verantwortliche im BCM auszuarbeiten, festzuhalten (wer macht was bis wann) und auf Umsetzung zu prüfen.

17.5. Bei nicht fristgerechter Umsetzung ist eine Eskalation unter Einbeziehung der Führungsebene durchzuführen.