



Schnell reagieren mit einem betrieblichen Kontinuitätsmanagement

Das Business Continuity Management System (BCMS) ist Bestandteil des allgemeinen Management Systems einer Organisation. Es stärkt mit seinen Maßnahmen die Resilienz und schafft durch regelmäßige Aktualisierung von Business Continuity Plänen (BCP) und ICT-Recovery-Plänen die Grundlagen für einen schnellstmöglichen Wiederanlauf der kritischen Geschäftsprozesse und der geschäftskritischen ICT. Darüber hinaus stellt es Methoden und Hilfsmittel zur Verfügung, um Krisen erfolgreich zu bewältigen.

Die Notwendigkeit zur Einführung eines BCMS kann aus diversen Bereichen resultieren und führt nach Umsetzung zu folgenden Mehrwerten:

-  Schadensreduktion durch Prävention
-  Identifikation kritischer Geschäftsprozesse und Services
-  Schutz gegen inakzeptable Ausfallzeiten
-  Vermeidung von Image- und Reputationsschäden
-  Erfüllung von Compliance Anforderungen
-  Reduktion von Haftungsrisiken
-  Marketing- und Wettbewerbsvorteil

DAS ZUSAMMENSPIEL DER VERSCHIEDENEN TEILE EINES BCMS

Das Business Continuity Management (BCM) kümmert sich im Kern um die Fortführung der kritischen Geschäftsprozesse. Heutzutage sind jedoch fast alle kritischen Geschäftsprozesse

abhängig von einer funktionierenden ICT. Längere Ausfälle von ICT-Infrastrukturen, ICT-Systemen oder IT-Anwendungen haben oft fatale Folgen für die Geschäftstätigkeit des Unternehmens bis hin zur Existenzbedrohung. Anforderungen an die Fortführung kritischer Geschäftsprozesse sind somit auch immer Anforderungen an die ICT Service Continuity. Durch ein etabliertes ICT Service Continuity Management (ITSCM) mit grundlegenden Elementen einer ICT-Notfallvorsorge und eine trainierte Reaktionsstruktur mit festgelegten Rollen sind Sie auf kritische IT-Vorfälle bestens vorbereitet. Die für die Fortführung des Geschäftsbetriebs benötigten ICT-Services werden nicht oder nur kurzzeitig beim Übergang in den Notbetrieb unterbrochen. Die wirtschaftliche Existenz bleibt auch bei größeren Schadensereignissen gewährleistet. Das Krisenmanagement (CM) fängt auf, was nicht planbar ist. BCM und ITSCM sind die proaktiven Komponenten des BCM Systems. Jedoch kommt es nicht selten vor, dass sich ein Notfall in eine Krise weiterentwickelt oder ein Ereignis bereits von Anfang an das Ausmaß einer Krise hat. Dies erfordert eine weiter greifende Herangehensweise. Dafür werden im Rahmen eines vollständigen BCMS die notwendigen Krisenpläne, Methoden und Hilfsmittel zur Lagebewältigung etabliert.

FOKUS AUF VERFÜGBARKEIT

Im Mittelpunkt der betrieblichen Notfallplanung steht die Verfügbarkeit der für das Unternehmen und dessen Zielerreichung kritischen Geschäftsprozesse inkl. aller hierfür erforderlichen Ressourcen. Dabei handelt es sich vielfach um die IT als offensichtlichste notfallrelevante Ressource. Aber auch alle anderen Ressourcen müssen im Fall eines widrigen Ereignisses gemäß den Verfügbarkeitsanforderungen aus den kritischen Geschäftsprozessen wieder bereit stehen. Gemeint sind hier Ressourcen wie z. B. Notbetriebspersonal, Notfallarbeitsplätze oder auch kritische Dienstleistungen. Daher sollten BCM und ITSCM immer Hand in Hand gehen

und einen ganzheitlichen, prozessorientierten Ansatz verfolgen. In Anlehnung an die Unternehmensziele und die Wertschöpfung werden die wesentlichen Prozesse und Ressourcen im Rahmen einer Business Impact Analyse (BIA) identifiziert. Die BIA enthält eine Bewertung der Prozesse und Ressourcen hinsichtlich der Anforderungen an die Verfügbarkeit und eine entsprechende Klassifikation der Kritikalität.

RISIKOORIENTIERTES VORGEHEN

Bezüglich der kritischen Prozesse und Ressourcen werden Risiken im Rahmen eines Risk Assessments (RA) identifiziert, welche zu einer schwerwiegenden Unterbrechung des Geschäftsbetriebes führen können. Basierend auf den Ergebnissen der Anforderungserhebung (=Business Impact Analyse, BIA) und der Risikosituation werden die individuellen Worst-Case-Szenarien abgeleitet. Anschließend werden BC- und ITSC-Lösungsoptionen (Strategien) je Szenario entwickelt. Diese bilden die Grundlage bei der Erstellung der Business Continuity Pläne (BCP) und ICT-Recovery Pläne.

PRIORISIERUNG DER KRITISCHEN GESCHÄFTSPROZESSE UND OPTIMALE FESTLEGUNG DES NOTBETRIEBSNIVEAUS

Wichtig für einen erfolgreichen Wiederanlauf in den Notbetrieb ist die richtige Priorisierung der Geschäftsprozesse anhand ihrer Kritikalität und Abhängigkeiten zu einander. Darüber hinaus sollte das erforderliche Notbetriebsniveau (MBCO) je Geschäftsprozess so konkret wie möglich festgelegt werden. Beide Informationen gewinnt man beispielsweise aus einer ordnungsgemäß durchgeführten BIA.

MANAGEMENTSYSTEME ALS ITERATIVER PROZESS

Der Aufbau und Betrieb eines BCMS stellt keinen einmaligen Prozess dar. Aktivitäten, wie BIA, RA, Anpassung der Lösungsoptionen und Notfallpläne sowie das Testen und Üben finden im Rahmen des BCMS-Lifecycles regelmäßig (jährlich) statt. Darüber hinaus sollte die oberste Leitung einer Organisation regelmäßig ein Managementreview auf die Wirksamkeit des BCMS durchführen und Verbesserungen initiieren.

WIRTSCHAFTLICHKEIT DURCH SCHNELLE REAKTIONSFÄHIGKEIT

Der proaktive Aufbau und die Schulung einer angemessenen Reaktionsstruktur (z.B. MoD, Krisenstab, Reaktionsteams, etc.) verhindern unnötigen Zeitverlust bei der Reaktion auf ein widriges Ereignis (Notfall, Krise, Katastrophe). Darüber hinaus helfen die vorab erarbeiteten Notfallpläne bei einem schnellen und koordinierten Wiederanlauf in den Notbetrieb sowie die

verfügbaren Ressourcen zielgerichtet einzusetzen. Durch eine schnelle und angemessene Reaktion können Schäden in den Bereichen Reputation, Finanzen, Verstöße gegen Regulatorik sowie schwerwiegende operative Auswirkungen vermieden werden.

DER INTEGRIERTE ANSATZ

Ein BCMS muss nicht als isoliertes Managementsystem entwickelt und betrieben werden. Es kann in eine bestehende Struktur von Managementsystemen (wie z.B. QMS, ISMS, RMS, etc.) integriert werden. Im Rahmen eines Integrierten Management Systems (IMS) stehen diese Managementsysteme parallel zu einander und es werden lediglich Synergien genutzt und Doppelarbeiten vermieden.

Darüber hinaus ist bei diesem Ansatz die Akzeptanz bei den Mitarbeitern höher, da sie nicht zum selben Thema von mehreren Seiten angesprochen werden. Ebenso ist der Ressourceneinsatz zum Betrieb der einzelnen Managementsysteme durch diesen Ansatz geringer.

NACHWEISBARKEIT DURCH ZERTIFIZIERUNG

Ein BCMS, welches konform zur internationalen Norm ISO 22301 implementiert ist, kann durch ein akkreditiertes Unternehmen zertifiziert werden. Ein Zertifikat bietet die Möglichkeit, ein funktionierendes BCMS gegenüber Dritten, wie z.B. Behörden, Wirtschaftsprüfern, Kunden und Partnern nachzuweisen.

UNSERE SERVICES

- Gap-Analysen zur aktuellen Standortbestimmung
- Analyse bestehender BCM und ITSCM Lösungen
- Konzeption und Implementierung eines BCMS nach ISO 22301 i.V.m. ISO 27031 oder nach BSI 200-4 sowie nach BCI GPG 2018
- Stellen eines externen BC Managers (eBCM)
- Durchführung von BIA und BCM Risk-Assessments
- Durchführen von ICT-Modellbildung und Gap-Analyse
- Coaching von BC-, ITSC- und Krisen-Managern
- Unterstützung bei der Auswahl und Implementierung eines geeigneten GRC-Tools
- Qualitätssicherung während des Projektes durch zertifizierte Expert*innen
- Unterstützung bei der Erstellung von Schulungskonzepten/-plänen sowie Durchführung von Schulungen
- Unterstützung bei Test-/ Übungsplanung, -Konzeption, -Durchführung und -Nachbereitung (Nachweise)

ANGEBOT ANFORDERN! 

TÜV Rheinland i-sec GmbH
Am Grauen Stein | 51105 Köln | Deutschland
cybersecurity@tuv.com
www.tuv.com/cybersecurity

 **TÜVRheinland®**
Genau. Richtig.