

Verschiedene Stufen für unterschiedliche Ansprüche

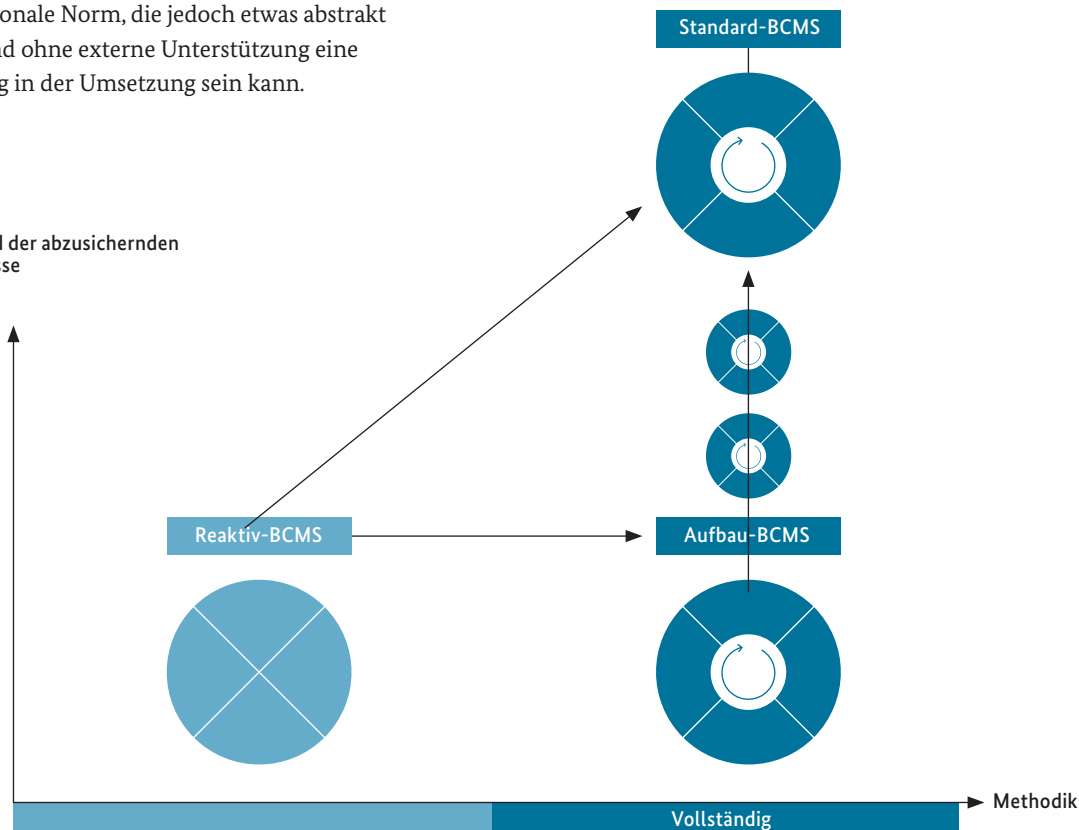
BCM als Thema und als Managementsystem ist in der Praxis häufig noch nicht so weit verbreitet wie Managementsysteme für Informationssicherheit (ISMS). Viele Institutionen stehen noch davor, sich selbst systematisch mit dem Thema Business Continuity zu beschäftigen und ein eigenes Business-Continuity-Management-System (BCMS) aufzubauen.

Gleichzeitig gibt es mit der **ISO 22301:2019** eine angesehene internationale Norm, die jedoch etwas abstrakt formuliert ist und ohne externe Unterstützung eine Herausforderung in der Umsetzung sein kann.

Abdeckungsgrad der abzusichernden Geschäftsprozesse

Vollständig

Eingeschränkt



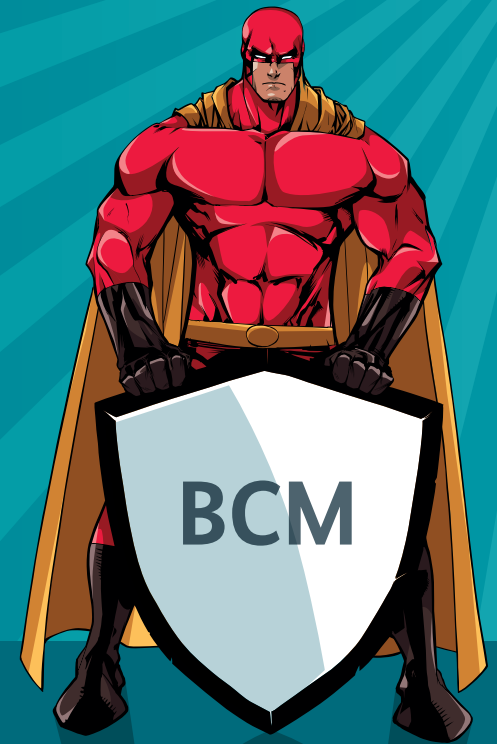
Daher wurde der BSI-Standard 200-4 als eine Umsetzungsanleitung formuliert und verfügt über ein Stufenmodell für die unterschiedlichen Voraussetzungen.

Er unterstützt Einsteiger durch die Einstiegsstufen Reaktiv- und Aufbau-BCMS dabei, ihr Business-Continuity-Management-System schrittweise aufzubauen.

Erfahrene Anwendende werden durch die Stufe Standard-BCMS angesprochen, die vollumfänglich mit der ISO 22301 kompatibel ist. Hier helfen ein Anforderungskatalog und Mapping auf die ISO-Norm bei der Umsetzung.

Business Continuity Management mit IT-Grundschutz

Wie man sich vor existenzbedrohenden Unterbrechungen des Geschäftsbetriebs schützen kann



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital • Sicher • BSI

Ausgangslage

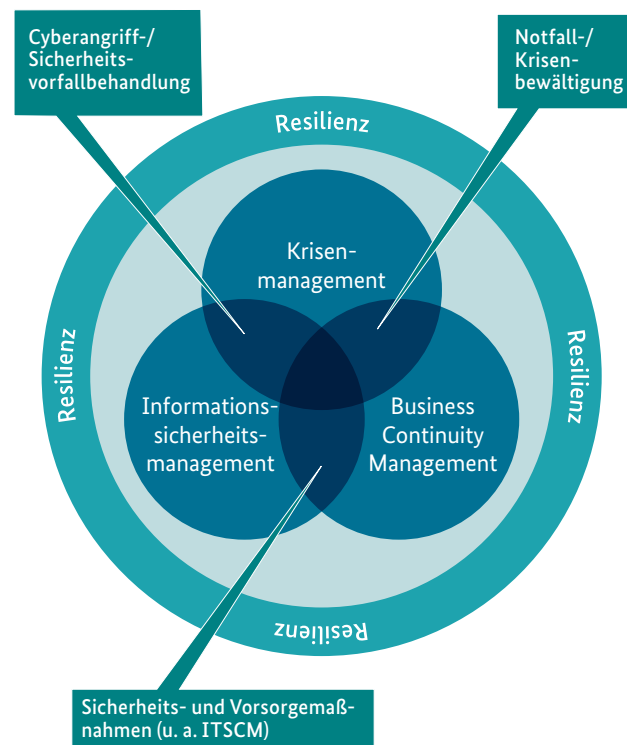
Ob der Ausfall eines Rechenzentrums, die Zerstörung einer Produktionsstätte infolge eines Naturereignisses oder eine Cyberattacke auf die gesamte IT-Infrastruktur – Institutionen sind einer **stetig wachsenden Bedrohungslage** ausgesetzt, die zu einer existenzbedrohenden Unterbrechung des Geschäftsbetriebes führen kann. Der BSI-Standard 200-4 Business Continuity Management (BCM) hilft, sich bestmöglich auf Schadensereignisse vorzubereiten.

Keine Insellösung, sondern Teil der organisatorischen Resilienz

Die Frage nach der Überlebensfähigkeit nach solchen Schadensereignissen bedarf dabei eines ganzheitlichen Blicks auf die gesamte Institution und alle möglichen Gefahren. Nur wenn Informationssicherheitsmanagement, Krisenmanagement und Business Continuity Management zusammenarbeiten, kann die organisatorische Resilienz nachhaltig gewährleistet werden (siehe nachfolgende Abbildung). Der BSI-Standard 200-4 stellt daher die wesentlichen Schnittstellen und Synergiepotentiale zu diesen Themen heraus und fügt sich nahtlos in die BSI-Standard-200 Reihe ein, die mit den BSI-Standards 200-1 Managementsysteme für Informationssicherheit, 200-2 IT-Grundschutz-Methodik und 200-3 Risikoanalyse auf der Basis von IT-Grundschutz Themen der Informationssicherheit adressiert.

Das **Krisenmanagement**, als dritte Säule der organisatorischen Resilienz, wird im BSI-Standard 200-4 neben dem **Business Continuity Management** grundlegend behandelt, sodass Institutionen auf Notfälle und Krisen unterschiedlichster Art vorbereitet sind.

BCM als integraler Bestandteil der organisatorischen Resilienz



Diese Abbildung soll das Zusammenspiel zwischen den drei Säulen der organisatorischen Resilienz aufzeigen. Die aufgeführten Schnittstellen zwischen diesen Themen werden im BSI-Standard ausführlich behandelt.

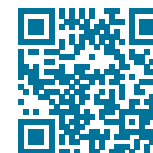
Unterstützung durch Hilfsmittel

Passend zum BSI-Standard 200-4 werden unterschiedlichste Hilfsmittel angeboten, die den Aufbau eines eigenen Business-Continuity-Management-Systems **erheblich vereinfachen** können.

Hierbei stehen **Dokumentvorlagen** für die verschiedenen BCM-Dokumente und **weitergehende** Informationen zu ausgewählten Fragestellungen zur Verfügung.

Weitere Informationen

Weitere Informationen zu BCM und dem BSI-Standard-200-4 finden Sie hier:



www.bsi.bund.de/gs-standard200-4

Impressum

Herausgeber: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Stand: September 2023

Druck: Appel und Klinger

Gestaltung: BSI

Bildnachweis: Titel: AdobeStock © Malchev