Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Glossar und Abkürzungsverzeichnis

BSI Standard 200-4

Änderungshistorie

Stand	*Version*	*Änderungen*
Dezember 2022	CD 1.0	Neukonzeption des Glossars mit integrierten Abkürzungsverzeichnis. Die Begriffe und Definitionen sind auf den CD 2.0 des BSI-Standards 200-4 abgestimmt
Dezember 2023	Final	Die Begriffe und Definitionen sind auf den finalen BSI-Standard 200-4 abgestimmt.

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik Postfach 20 03 63
53133 Bonn
Tel: +49 228 99 9582-5369
E-Mail: it-grundschutz@bsi.bund.de
Internet: https://www.bsi.bund.de

1 Abkürzungsverzeichnis

Abkürzung	Begriff
AAO	Allgemeine Aufbauorganisation
BAO	Besondere Aufbauorganisation
BC	Business Continuity
BCM	Business Continuity Management (deutsch: Notfallmanagement)
BCB	Business Continuity Beauftragte
BCK	Business Continuity Koordinierende
BCMS	Business Continuity Management System
BIA	Business Impact Analyse
BOS	Behörden und Organisationen mit Sicherheitsaufgaben
FOR-DEC	Facts, Options, Risks (and Benefits) – Decision, Execution, Check
GFP	Geschäftsfortführungsplan
ITSCM	Information Technology Service Continuity Management (deutsch: IT-Notfall-management)
LÜKEX	Ressort- und Länderübergreifende Krisenmanagementübung/Exercise
MBCO	Minimum Business Continuity Objective (deutsch: Notbetriebsniveau)
MTA	Maximal tolerierbare Ausfallzeit (siehe Definition Maximum Tolerable Period of Disruption)
MTPD	Maximal Tolerable Period of Disruption (deutsch: maximal tolerierbare Ausfallzeit)
NuK-Kommunikation	Notfall- und Krisen-Kommunikation
OE	Organisationseinheit
PDCA	Plan – Do – Check – Act
RPA	Recovery Point Actual (deutsch: Zugesicherter maximaler Datenverlust)
RPO	Recovery Point Objective (deutsch: maximal zulässiger Datenverlust)
RTA	Recovery Time Actual (deutsch: erreichbare Wiederanlaufzeit)
RTO	Recovery Time Objective (deutsch: geforderte Wiederanlaufzeit (WAZ))
SPoF	Single Point of Failure
WAP	Wiederanlaufplan
WAZ	Wiederanlaufzeit
WHP	Wiederherstellungsplan

Tabelle 2: Abkürzungsverzeichnis

2 Glossar

Das vorliegende Glossar bestimmt Fachbegriffe, die im BSI-Standard 200-4 BCM verwendet werden. Hier werden einige Begriffe aus den anderen BSI-Glossaren (Glossar der Cybersicherheit sowie IT-Grundschutz Glossar) aufgegriffen und in Bezug auf BCM konkretisiert.

Das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) definiert manche Begriffe anders als das BSI mit dem vorliegenden Glossar. Während der BSI-Standard 200-4 BCM thematisiert,-wie-Institutionen ihre Geschäftsfähigkeit in Notfallsituationen aufrechterhalten können, erfasst das BBK darüber hinaus weitere Themenfelder. Zu diesen zählen beispielsweise der Bevölkerungs- und Katastrophenschutz sowie der Zivilschutz. Das BBK fasst daher auch einige Definitionen deutlich weiter. Solche unterschiedlichen Definitionen gleichlautender Begriffe sind nicht im Gegensatz zu sehen, sondern ergänzen sich.

Jede Begriffsdefinition in diesem Glossar, die von Definitionen in den beiden anderen BSI-Glossaren oder in weiteren einschlägigen Werken abweicht, ist jeweils deutlich durch einen Hinweis gekennzeichnet.

Begriff	**Definition**
Alarmierung	Handlungsschema, in dem verantwortliche Entscheidende und Akteure möglichst schnell-benachrichtigt und in Einsatzbereitschaft versetzt werden
Allgemeine Aufbauorganisation (AAO)	ständige Organisationsform, in der die täglichen Aufgaben einer Institution nachfolgenden Kriterien strukturiert sind: • hierarchischer Aufbau • Zuständigkeiten • Kommunikations- und Entscheidungswege
Besondere Aufbauorganisation (BAO)	zeitlich begrenzte Organisationsform für umfangreiche und komplexe Aufgaben, insbesondere für Maßnahmen aus besonderen Anlässen, die im Rahmen der AAO nicht bewältigt werden können In dieser Organisationsform gelten temporäre Zuständigkeiten, Hierarchien sowie Kommunikations- und Entscheidungswege, die vom Normalbetrieb abweichen. (siehe Definition Führungsorganisation in Feuerwehr-Dienstvorschrift FwDV 100, Ziff. 3.2)
Business Continuity (BC)	(deutsch: Geschäftsfortführung) Fortführung oder Wiederaufnahme aller zeitkritischen Geschäftsprozesse nach Schadensereignissen, um die Arbeitsfähigkeit und die wirtschaftliche Existenz einer Institution zu sichern
Business Continuity Management (BCM)	Steuerung sämtlicher Aktivitäten, die eine geordnete Geschäftsfortführung nach Schadensereignissen zum Ziel haben Zu unterscheiden sind zwei wichtige Bereiche: 1. Vorsorge (Geschäftsprozesse sollten möglichst nicht unterbrochen werden.) 2. Reaktion (Geschäftsprozess sollten nach einem Ausfall in angemessener Zeit wieder hergestellt werden.)
Business Continuity Management System (BCMS)	Strukturen, Regeln und Aufbau innerhalb einer Institution, um eine geordnete Geschäftsfortführung nach Schadensereignissen in der Institution zu erreichen

Begriff	Definition
Business Continuity Strategie (BC-Strategie)	strukturierte strategische Lösungsansätze, wie die BC-Planung allgemein gestaltet und umgesetzt werden kann
Business Continuity-Lösung (BC-Lösung)	Maßnahme, die präventiv erarbeitet und umgesetzt wird, um eine Geschäftsfortführung im Notfall zu ermöglichen
BC-Planung	Gesamtheit aller BC-Lösungen und der vorbereitenden Planung der BAO
BC-Beauftragte (BCB)	(auch Business Continuity Managende, Notfallmanagende oder Notfallbeauftragte) Person, die für den Aufbau, den Betrieb und die kontinuierliche Verbesserung des BCMS zuständig ist
BC-Koordinierende (BCK)	Person, die in ihrem Zuständigkeitsbereich als fachliche Ansprechperson und Multiplikator oder Mulitplikatorin fungiert und die Umsetzung der Vorgaben zum BCM sicherstellt
BC-Konzept	Notfallvorsorgekonzept und Notfallhandbuch
Business Impact Analyse (BIA)	strukturierte Untersuchung mit dem Ziel, (zeit-)kritische Geschäftsprozesse und Ressourcen (Assets) zu identifizieren Hierzu werden diejenigen direkten und indirekten potentiellen Folgeschäden für die Institution ermittelt, die durch den Ausfall von Geschäftsprozessen verursacht werden. Daraus werden die Anforderungen an den Wiederanlauf von Geschäftsprozessen abgeleitet.
FOR-DEC	sechsstufiger Handlungszyklus, um schnelle und sachorientierte Entscheidungen in komplexen Umfeldern treffen zu können, der mit einer Bestandsaufnahme beginnt: "Facts", "Options", "Risks and Benefits“ „Decision", "Execution", "Check" (Fakten, Handlungsoptionen, Risiken & Nutzen der Handlungsoptionen Entscheidung, Ausführung, Kontrolle)
Gefahr	(siehe Gefahr, Glossar im IT-Grundschutz-Kompendium zum Zeitpunkt der Veröffentlichung) (Bitte beachten: Das BBK definiert diesen Begriff anders.)
Gefährdung	(siehe Gefährdung, Glossar im IT-Grundschutz-Kompendium zum Zeitpunkt der Veröffentlichung) (Bitte beachten: Das BBK definiert diesen Begriff anders.)
Geschäftsfortführungsplan (GFP)	Plan, der dokumentiert, wie eine Institution auf der Prozessebene auf eine Geschäftsunterbrechung nach einem Ressourcenausfall reagiert
Krise	Schadensereignis, das sich in massiver Weise negativ auf eine Institution auswirkt und dessen Auswirkungen 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. (siehe auch Krisenmanagement) (Bitte beachten: Das BBK definiert diesen Begriff anders.)

Begriff	Definition
Krisenbewältigung	alle Tätigkeiten die dazu dienen, eine Krise nach Eintritt zu bewältigen
Notfall- und Krisen-Kommunikation	Tätigkeiten, die vor oder während einer Krise oder einem Notfall und gegebenenfalls auch nach deren Bewältigung ausgeführt werden, um relevante Informationen zu sammeln, zu verifizieren sowie zielgruppengerecht nach innen und außen zu kommunizieren Für die Notfall- und Krisenkommunikation werden vorab entsprechende Konzepte zum Umgang mit den verschiedenen Interessengruppen, z. B. den Mitarbeitenden und-den Medien erarbeitet. Falls nötig werden diese Konzepte im Rahmen der Bewältigung angepasst und fortlaufend überarbeitet.
Krisenmanagement	(siehe Glossar der Cyber-Sicherheit, BSI) (Bitte beachten: Im Rahmen des BSI-Standards 200-4 bezieht sich der Begriff lediglich auf institutionsinterne Krisen, d. h. ist enger gefasst als im Zusammenhang mit der öffentlichen Gefahrenabwehr, z. B. durch die Feuerwehr (siehe FwDV 100))
Lage	zielgruppenspezifische, sachliche und auf die wesentlichen Aspekte reduzierte Beschreibung der vorliegenden Situation Die Beschreibung gliedert sich in: - die allgemeine Lage (äußere Rahmenbedingungen) - die Schadenslage (konkreter Schaden) - die eigene Lage (konkrete Situation der betrachteten Institution) Die Schadenslage und die eigene Lage können sich inhaltlich überschneiden. (Bitte beachten: angelehnt an den Führungsvorgang, FwDV 100)
Lagebild	Ergebnis der Aufbereitung von Informationen zu einem Schadensereignis in textlicher und oder visualisierter Form (siehe auch Lagekarte und Lagedarstellung, FwDV 100)
Maximum Acceptable Outage (MAO)	(siehe Maximum Tolerable Period of Disruption)
Maximum Data Loss (MDL)	(siehe: Recovery Point Objective)
Maximum Tolerable Period of Disruption (MTPD)	auch MTPoD (deutsch: maximal tolerierbare Ausfallzeit (MTA)) zeitliche Obergrenze bis zu der ein Geschäftsprozess maximal ausfallen darf, bevor nicht tolerierbare Auswirkungen für eine Institution auftreten Die Obergrenze wird anhand einer Schadensbewertung des betreffenden Geschäftsprozesses ermittelt.
Medienmonitoring	(deutsch: Medienbeobachtung) Überwachung und Analyse aller Kommunikation im Umfeld der Institution mit den folgenden Zielen: • (Früh-)Erkennung von Ereignissen mit Krisenpotenzial (insbesondere Kommunikationskrisen) • Verbesserung der Kommunikation während der Bewältigung und Nachbereitung von Notfällen und Krisen

Begriff	Definition
Minimum Business Continuity Objective (MBCO)	(siehe Notbetriebsniveau)
Normalbetrieb	planmäßiger Geschäftsbetrieb einer Institution
Notbetrieb	nach einem Schadensereignis stattfindender, gegebenenfalls eingeschränkter, Geschäftsbetrieb, der die erforderlichen sowie zeitkritischen Funktionen der betroffenen Geschäftsprozesse sicherstellt
Notbetriebsniveau	(engl. Minimum Business Continuity Objective oder MBCO) erforderliche Leistungsfähigkeit im Notfall, um einen angemessenen Geschäftsbetrieb gewährleisten zu können Das Notbetriebsniveau wird je Geschäftsprozess oder Ressource individuell festgelegt.
Notfall	Unterbrechungen mindestens eines-zeitkritischen Geschäftsprozesses, 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 ist ein Notfall ein Schadensereignis für dessen Bewältigung entweder geeignete Pläne vorliegen oder bestehende Pläne adaptiert werden können. 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. (Bitte beachten: Das BBK definiert diesen Begriff anders.)
Notfallbeauftragte	(siehe BC-Beauftragte)
Notfallbewältigung	alle institutsinternen Tätigkeiten, die dazu dienen, nach Eintritt eines Notfalls • in einen Notbetrieb zu gelangen, • den Notbetrieb aufrechtzuerhalten und • wieder in den Normalbetrieb zu gelangen
Notfallhandbuch	Dokument mit allen Informationen, die für die Notfallbewältigung benötigt werden Das Dokument umfasst-z. B.-alle Notfallpläne, die Geschäftsordnung des Stabes und das Kommunikationskonzept.
Notfallkonzept	(siehe BC-Konzept)
Notfallmaßnahmen	alle Maßnahmen, die präventiv erarbeitet und bei Eintritt eines Notfalls umgesetzt werden, um den Schaden zu begrenzen und Geschäftsprozesse fortzuführen
Notfallpläne	Dokumente innerhalb des Notfallhandbuchs, mit denen planbare Ereignisse innerhalb eines vorab definierten Notbetriebs bewältigt werden können Zu diesen Dokumenten zählen z. B. die Geschäftsfortführungs-, Wiederanlauf- und Wiederherstellungspläne.
Notfallplanung	(siehe BC-Planung)

Begriff	Definition
Notfallvorsorge	alle präventiven Maßnahmen und Verfahren, die vor dem Eintritt eines Schadensereignisses durchgeführt werden (Bitte beachten: Das BBK definiert diesen Begriff anders.)
Organisationseinheit	logische Einheit einer Institution, z. B. ein Standort, eine Abteilung, oder ein Fachbereich
Prozesskette	eine Reihe von mehreren, untereinander abhängigen Geschäftsprozessen, z. B. Auftragseingang, Herstellung, Lieferung, Abrechnung Die Reihe als Ganzes trägt zur Wertschöpfung in einem Unternehmen oder zur Erfüllung des öffentlichen Auftrages einer Behörde bei.
Recovery Point Actual (RPA)	(deutsch: tatsächlicher zu erwartender Datenverlust) tatsächlicher, zu erwartender Datenverlust im Falle eines Schadensereignisses Die RPA wird in der Regel als tatsächlicher Datensicherungszyklus je Anwendung, IT-System oder Geschäftsprozess angegeben.
Recovery Point Objective (RPO)	(deutsch: maximal zulässiger Datenverlust) Wert für das Alter, das verfügbare Daten maximal haben dürfen, um zeitkritische Geschäftsprozesse nach einer Unterbrechung sinnvoll betreiben zu können Der maximal zulässige Datenverlust wird in der Regel als geforderter Datensicherungszyklus je Anwendung, IT-System oder Geschäftsprozess angegeben.
Recovery Time Actual (RTA)	(deutsch: tatsächliche zu erwartende Wiederanlaufzeit, tatsächliche WAZ) beschreibt den Zeitraum vom Ausrufen des Notfalls bis zum Zeitpunkt der tatsächlichen Inbetriebnahme der Notfall-Lösung, z. B. durch Schwenk auf eine Ausweich- oder Ersatzressource
Recovery Time Objective (RTO)	(deutsch: geforderte Wiederanlaufzeit, geforderte WAZ) beschreibt den Zeitraum vom Ausrufen des Notfalls bis zum Zeitpunkt der geforderten Inbetriebnahme der Notfall-Lösung, z. B. durch Schwenk auf eine Ausweich- oder Ersatzressource.
Ressource (Geschäftsprozess)	alle physischen und digitalen Werte, die erforderlich sind, um Geschäftsprozesse durchführen zu können Werte im betriebswirtschaftlichen Sinn sind z. B. Personal, IT-Systeme, Gebäude, Dienstleistungsunternehmen, Maschinen oder Betriebsmittel.
Schaden	(angelehnt an IT-Grundschutz-Glossar, BSI) (Bitte beachten: Das BBK definiert diesen Begriff anders.)
Schadensereignis	Vorfall, der zu einer Abweichung von einem erwarteten Ergebnis führt (Bitte beachten: Das BBK definiert diesen Begriff anders.)
Service Level Agreement (SLA)	eine Vereinbarung zwischen zwei Parteien, die festschreibt, welche exakten Eigenschaften, z.B. Schnittstellen, Leistungsniveau und Gütestufen, eine Leistung erreichen soll
Störung	eine Situation, in der Prozesse oder Ressourcen nicht wie vorgesehen zur Verfügung stehen oder funktionieren

Begriff	Definition
	So bezeichnet werden Situationen, die in der Regel innerhalb des Normalbetriebs durch die Allgemeine Aufbauorganisation der Institution behoben werden können. Hierzu wird auf vorhandene Prozesse zur Störungsbeseitigung oder des Incident-Managements zurückgegriffen.
Störungsbehandlung	Vorgehen (z. B. Prozesse) einer Institution, um Störungen im Normalbetrieb zu beheben
Wiederanlauf	alle Maßnahmen, um strukturiert in einen (vorab geregelten) Notbetrieb wechseln zu können
Wiederanlaufplan (WAP)	Dokumentation, die beschreibt, wie eine Institution ausgefallene Ressourcen, z. B. durch umgesetzte Business-Continuity-Lösungen oder Ersatzlösungen, kompensieren kann Ziel der Kompensation ist ein Notbetrieb, der die Geschäftsfortführung sicherstellt.
Wiederanlaufzeit (WAZ)	Es wird unterschieden zwischen • geforderte Wiederanlaufzeit (siehe RTO) und • tatsächliche Wiederanlaufzeit (siehe RTA).
Wiederherstellung	geordnete Rückkehr in einen Zustand, in dem der Normalbetrieb wieder möglich ist
Wiederherstellungsplan (WHP)	Dokumentation, die beschreibt, wie ausgefallene Ressourcen in den Normalbetrieb zurückversetzt werden können
Vorsorgemaßnahme	alle Maßnahmen, die präventiv erarbeitet und umgesetzt werden und die Wahrscheinlichkeit eines Ressourcenausfalls reduzieren
zeitkritisch	Einordnung für alle Geschäftsprozesse oder Ressourcen, deren Ausfall innerhalb eines zuvor festgelegten Zeitraums zu einem nicht tolerierbaren, unter Umständen existenzgefährdenden Schaden für eine Institution führen kann. Die Einordnung von Ressourcen wird dabei von der Einordnung der Geschäftsprozesse, die die jeweiligen Ressourcen benötigen, abgeleitet.

Tabelle 3: Glossar