Die ISO 22301:2012 stellt die neue, zentrale Richtlinie der International Organization for Standardization (ISO) für ein Business Continuity Management dar.

Die Norm ist eine Fortsetzung der vom ISO-Institut herausgegebenen generischen Normen, wie beispielsweise die ISO 31000 (Risikomanagement) oder die ISO 27001 (Informationssicherheit-Managementsysteme). Damit kann sie für Unternehmen jeder Größe und unabhängig von der vorhandenen Technologie angewandt werden. Die ISO 22301 kann Organisationen in den Genuss der Vorteile eines strukturierten betrieblichen Kontinuitätsmanagements bringen.

Vorteile:

- Organisationsweit einheitliche Steuerungs-möglichkeit und nachvollziehbare Ergebnisse
- Schaffung von Transparenz über die kritischen Geschäftsprozesse, deren Abhängigkeiten und potentiellen Risiken sowie der Risikobehandlung
- Kostenreduktion durch effiziente und schnelle Reaktion auf Vorfälle
- Compliance mit internen und externen Vorgaben und Regelungen

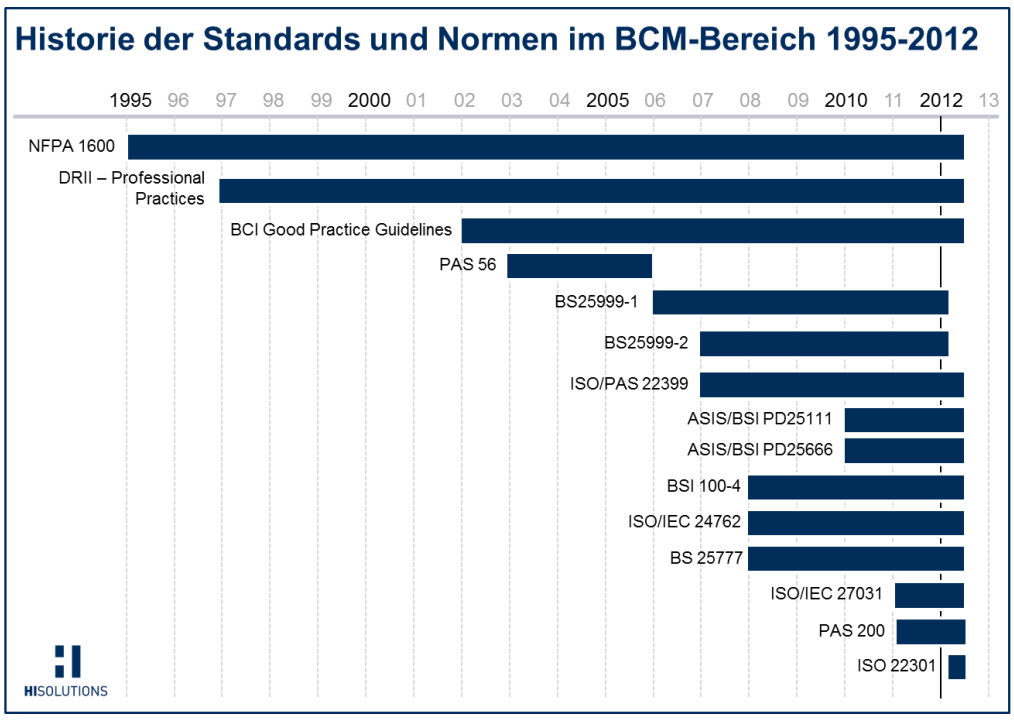
Historische Entwicklung der Standards und Normen

Business Continuity Management (BCM) ist ein seit mittlerweile mehr als 15 Jahre geprägter Begriff. BCM wird professionell bereits seit Mitte der 90er Jahre, beginnend mit der Verwendung einheitlicher Vorgehensweisen eingesetzt und entwickelt.

Im November 2006 wurde vom British Standards Institute der British Standard 25999-1 „Business Continuity Management – Part 1: Code of Practice“ als erster offizieller Standard für den Aufbau eines Managementsystems für das betriebliche Kontinuitäts-management veröffentlicht. Dieser enthält unter anderem Anforderungen für den Aufbau einer Organisationsstruktur, die Umsetzung eines Business Continuity Management-Prozesses auf Basis von Good Practice Vorgaben und die Konzeption organisatorischer Maßnahmen. Die detaillierten Arbeitsschritte oder konkreten Maßnahmen für ein Business Continuity Management System (BCMS) werden nicht beschrieben. Dafür wird im BS25999-1 auf weitere Normen der ISO-Reihe wie ISO 9000 oder ISO 27001 bzw. den PAS77 verwiesen.

Dazu veröffentlichte das British Standards Institute in 2007 den Standard BS 25999-2 „Business Continuity Management – Part 2: Specification“, welcher die Punkte, die zur Zertifizierung eines BCMS vorhanden sein müssen, umfasst. Dieser war allerdings nur verbindlich vorgeschrieben für Großbritannien, wurde jedoch weltweit angewandt.

Mit der Veröffentlichung der ISO 22301 in 2012 gibt es nun erstmals eine international gültige Norm. Die Highlights daraus werden nachfolgend beschrieben.



Die ISO 22301 – Wrap-up und Neuerungen

Die ISO 22301 ist die erste international anerkannte Norm für BCM-Systeme.
Sie hebt insbesondere die Anforderung an Unternehmen hervor, ein Managementsystem aufzusetzen, das Business Continuity auf der obersten Geschäftsführungsebene ansiedelt, die erforderlichen Ressourcen zur Verfügung stellt und regelmäßig überprüft.

Die Norm ist technologie- und herstellerneutral verfasst und somit anwendbar für Unternehmen jeder Größe, welche ihr Business Continuity Management verbessern wollen, mit folgenden möglichen Zielen:

- Etablieren, Einführen, Monitoren und Verbessern eines BCMS.
- Sicherstellen der Compliance mit den internen Regelungen sowie externen Anforderungen.
- Erreichen eines zertifizierten BCMS.

Zentrale Säulen der neuen ISO 22301 sind die Bereiche der Planung eines BCMS, Kommunikation und Monitoring sowie die Formulierung eindeutiger Anforderungen an das Management.

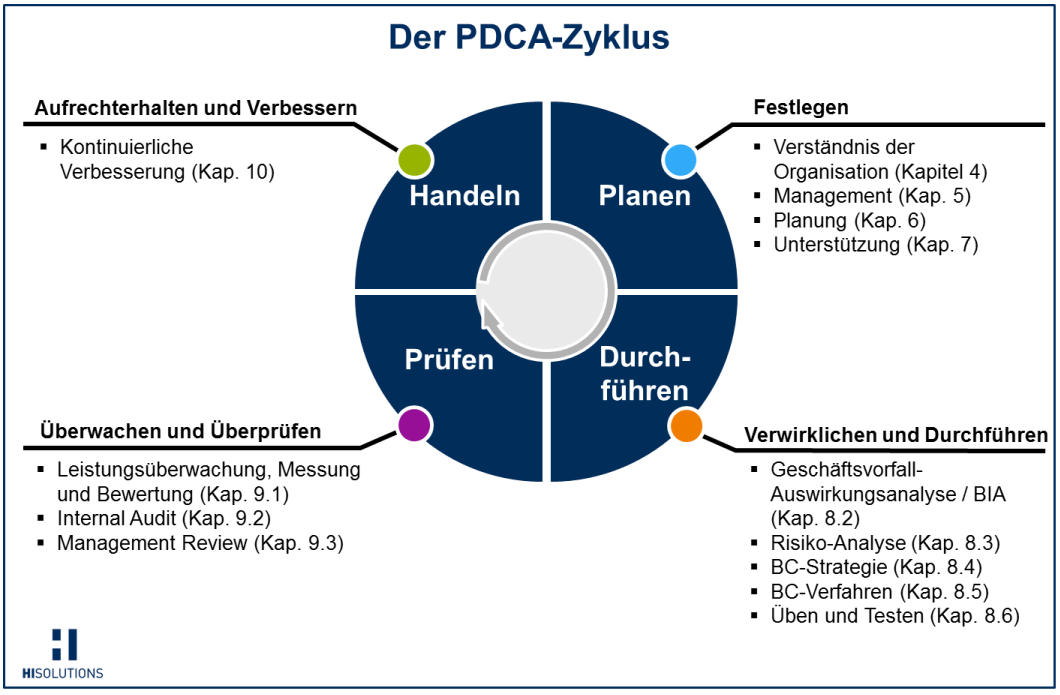
Im Speziellen wird jetzt die Einbindung in das zentrale Risikomanagement mit Anforderungen an mehreren Stellen unterlegt.

Darüber hinaus wird explizit der Aufbau von Metriken für die Messbarkeit der Erreichung der Ziele des BCMS gefordert. Die ermittelten Ergebnisse ermöglichen zudem Rückschlüsse auf die Erreichung der Unternehmensziele.

Die ISO 22301 ist in zehn Kapitel unterteilt, welche den altbekannten BCM Life-Cycle weitgehend abbilden. Explizit dargestellt wird dieser aber nicht mehr.

Kapitel 4 beschreibt den äußeren Ring „Embedded in the organization's culture". Das zentrale Programmmanagement ist auf die Kapitel 6 und 7 aufgeteilt.

Nach wie vor vorhanden ist das PDCA-Modell (Plan-Do-Check-Act) als zentrale Vorgehensweise für Festlegung, Verwirklichung und Durchführung (Betrieb, Übung), Überwachung und Überprüfung sowie Aufrechterhaltung und Verbesserung der Wirksamkeit des BCMS einer Organisation.



Neue Terminologie

In der neuen ISO-Norm sind einige neue Begriffsdefinitionen hinzugekommen. Die wesentlichsten Veränderungen stellen dar:

Korrigierende Aktivität
beschreibt die Aktivität, die notwendig ist, die Ursache einer Nicht-Konformität zu beheben und sicherstellen, dass diese nicht wieder auftritt.

Dokumentierte Information
beschreibt alle für das BCMS erforderlichen Informationen, die vom Unternehmen aufgenommen, überwacht und gewartet werden müssen sowie das Medium, auf dem es gespeichert ist.

Maximaler Datenverlust (RPO)
beschreibt den Zeitpunkt, bis wann eine Information wiederhergestellt sein muss, um eine Wiederaufnahme der Aktivitäten zu gewährleisten (=maximal zulässiger Datenverlust).

Mindestziel des Notfallmanagements (MBCO)
beschreibt das Mindestlevel, das für eine Dienstleistung oder ein Produkt während einer Unterbrechung bzw. Störung gewährleistet sein muss, damit das Unternehmen seine Geschäftsziele erreicht.

Im Vorfeld wurden in den BCM-Foren speziell bei der festen Definition der Termini des maximal tolerierbaren Datenverlusts sowie der Ausfallzeitspannen und Wiederherstellungszeiten kontroverse Diskussionen über deren Verwendung in der neuen ISO 22301 geführt.

Auf dem Expertenforum des Business Continuity Institute (BCI) und British Standards Institute wurde jedoch noch einmal herausgestellt, dass die ISO 22301 als generische Norm nicht die verbindliche Verwendung spezieller Termini vorschreiben kann. Es wurden eingangs zwar Definitionen dargestellt. In den Einzelkapiteln wurden allerdings keine Abkürzungen mehr verwendet, eher wurde der Fokus auf die Beschreibung der Vorgehensweise gelegt. Eine detaillierte Erläuterung der Begriffe und Zuordnung zu den Beschreibungen der ISO 22301 ist in der ISO 22313 vorgesehen, welche voraussichtlich Anfang 2013 veröffentlich wird.

Darüber hinaus wurde betont, dass in den Organisationen teilweise eigene Begrifflichkeiten eingesetzt werden. Der Fokus soll auf der Erfüllung der Anforderungen liegen, unabhängig von den gewählten Begriffen.

Wesentliche Bereiche

Zugrundeliegendes Dokument stellt der bekannte BS25999-2 dar. Formuliert ist die neue Norm ISO 22301 in den Konventionen der ISO, in denen auch bereits Normen anderer Bereiche, bspw. ISO 27001 (Informationssicherheit-Managementsysteme) verfasst sind.

Im BS25999-2 wurde im Kapitel 4„Understanding the Organisation“ in erster Linie die Durchführung der Business Impact Analyse und der Risikoanalyse gesehen. In der neuen Norm wird in dem extra vorangestellten **Kapitel 4 „Verständnis der Organisation“** explizit Kenntnis der Organisation und des Umfeldes, in dem sie operiert, gefordert. Der wesentliche Fokus liegt auf den Fragestellungen zur vollständigen Identifikation und Dokumentation von:

- allen Aktivitäten, Aufgaben, Dienstleistungen, Produkte, Partnerschaften, Lieferketten (Supply Chain), sonstigen Stakeholdern sowie möglichen Auswirkungen einer Betriebsunterbrechung,
- allen Verknüpfungen zwischen der Business-Continuity-Strategy und -Politik und den Unternehmenszielen der Organisation sowie die Abhängigkeit zu anderen Regelwerken (inklusive. der Einbindung in die unternehmensübergreifende Risikomanagementstrategie),
- der Risikoakzeptanz im Unternehmen,
- allen Compliance-Anforderungen (extern, intern, regulatorisch), die für die Zielerreichung der Organisation relevant sind.

Darüber hinaus ist die Festlegung des Geltungsbereichs Teil dieses Kapitels.

Allen Änderungen in der neuen ISO-Norm voran wurde die **oberste Verantwortlichkeit des Managements** stärker in den Vordergrund gestellt als bei vergleichbaren Standards bzw. Normen zuvor. Hierzu wurde ebenfalls ein gesondertes Kapitel geschaffen (**Kapitel 5**), in welchem die Anforderung an das Top Management in vier Unterkapiteln definiert ist.

Neben dem bisherigen Commitment des Managements zur BCM-Policy sowie der Zuweisung der Steuerungs- und Umsetzungsverantwortung liegt nun beim obersten Management die Aufgabe, sicherzustellen, dass für alle relevanten Funktionen und Ebenen Unternehmensziele definiert sind, mit denen die BCM-Strategie einhergeht.

Ebenfalls als Managementaufgabe ist der **Management Review** in der neuen Norm unter **Kapitel 9.3** auch weiter verbindlich zu erbringen. Unverändert ist die Anforderungen an eine **interne Revision** (**Kapitel 9.2**).

Parallel rückt allerdings der Bereich **Leistungsüberwachung** (**Kapitel 9.1**) als nächste größere Änderung verstärkt in den Vordergrund. Nach der Implementierung eines BCMS müssen Maßnahmen zur periodischen Überwachung und Bewertung umgesetzt sein. Darunter fallen die Messbarkeit der abgestimmten Maßnahmen und Aktivitäten sowie die darauffolgende Ergebnisanalyse ebenso wie die Messung des Erreichungsgrad der BCM-Ziele gegen die Unternehmensziele. **Kapitel 9** fällt vollständig in den Bereich „Check“ des PDCA-Zyklus.

Als weiteren Bereich der Planungsphase fokussiert **Kapitel 6** die **Planung** des betrieblichen Kontinuitätsmanagements. Diese Phase stellt einen zentralen Schritt dar, da die Definition der strategische Ziele und Leitprinzipien das Fundament für das BCM bildet.

Kriterien für Business-Continuity-Ziele:

- Konsistenz mit Business-Continuity-Strategie bzw. –Politik
- Messbarkeit
- Beachtung von anwendbaren Anforderungen
- Überwachung, gegebenenfalls Aktualisierung der BC-Ziele

Als letzten Bereich der Planung erfolgt die Festlegung der Unterstützungsprozesse. Dabei werden unter **Support** in **Kapitel 7** die zur Umsetzung des BCMS benötigten Anforderungen an die Resourcenplanung, Schaffung von Mitarbeiterkompetenzen und eine allgemeine Mitarbeiter-Awareness definiert.

Dazu kommt dem **Kommunikations- (Kapitel 7.4) und Dokumentationssystem** (**Kapitel 7.5**) ein größerer Fokus zu als im BS25999-2. Es müssen Prozesse bzw. Verfahren für die:

- interne und externe Kommunikation
- Verfügbarkeit der Kommunikationswege
- Kommunikation mit offiziellen Behörden / Stellen
- Notfallkommunikationswege und -medien

eingeführt und geleitet werden.

Alle Themenbereiche der Planung müssen in einer angemessenen Dokumentationsstruktur verwaltet werden. Hierzu wurde die neu hinzugefügte Terminologie der *dokumentierten Information* (**Kapitel 7.5**) integriert. Darunter werden alle Maßnahmen zur Entdeckung und regelmäßigen Überwachung von Zwischenfällen sowie zur Sicherstellung der Aktualität und Zugriffsbereitschaft auf die Kommunikationswege und -medien gefasst. Ein Change-Management-Prozess für die wesentlichen Dokumente ist ebenfalls zu etablieren.

Der Dokumentationsaspekt wird auch im **Kapitel 8.4.3** als Teil der Umsetzung der BC-Verfahren noch einmal deutlicher als im BS25999-2 herausgestellt. Damit erhält die Kommunikation und das Dokumentenmanagement eine hervorstehende Rolle mit ganz präzisen Anforderungen.

Die Umsetzung bzw. Durchführung des Business Continuity Managementsystems ist in **Kapitel 8 „Operation“** ausführlich beschrieben. Hier werden detailliert alle einzelnen Phasen und Schritte der BCM-Umsetzung mit Anforderungen unterlegt.

In diesem Bereich sind vor allem:

- die Business Impact Analyse
- (als Prozess zur Identifikation kritischer Geschäftsbereiche und deren Abhängigkeiten im Hinblick auf Ausfallszenarien)
- die Risikoanalyse
- (mit dem Verweis auf die hierfür vorhandene ISO-Norm 31000)
- die Ableitung von BC-Strategien
- die Erstellung von BC-Verfahren und
- das Üben und Testen

hervorzuheben.

Im abschließenden **Kapitel 10** „**Verbesserung**“ sind mit den Anforderungen an einen kontinuierlichen Verbesserungsprozess alle Prozesse subsummiert, welche die Effizienz (optimales Kosten-Nutzen-Verhältnis) und Wirksamkeit (Erreichung der Ziele) der Sicherheitsprozesse und Kontrollsysteme abbilden, Ziel sollte es sein, die Effizienz und Wirksamkeit des BCMS kontinuierlich zu steigern.

Zertifizierungsvorgang und Übergangsphase

Mit Veröffentlichung der ISO 22301 im Mai 2012 wurde gleichzeitig das Ende der BS25999-2 Zertifizierungen eingeläutet.

Bis November 2012 können sich Unternehmen noch offiziell gegen den BS25999-2 zertifizieren lassen. Die Zertifikate sind maximal bis Mitte 2014 gültig.

Gleichzeitig startete mit der Veröffentlichung der ISO 22301 die Upgradephase, in der BS25999-2-zertifizierte Unternehmen auf die neue ISO 22301 umstellen können.

Die für die bisherigen Zertifizierungen vorhandenen Anleitungen bzw. Beschreibungen des Zertifizierungsstandards (wie bspw. der BS25999-1 für die BS25999-2 Zertifizierung) werden ebenfalls aktualisiert. Hierzu wird in 2013 die ISO 22313 als begleitendes Dokument erscheinen, in welchem Erläuterungen und Beispiele zu den Anforderungen der ISO 22301 gegeben werden. Es ist zwar nicht erforderlich, aber durchaus empfehlenswert, mit einem Upgrade auf die ISO 22301 bis zur Veröffentlichung der ISO 22313 zu warten, um evtl. Missverständnisse zu vermeiden.

Für die BS25999 Lead-Auditoren wird es gemäß Auskunft vom British Standards Institute eine zweitätige Schulung zur Überleitung auf die ISO 22301 geben.

Zusammenfassung

Als erste internationale Norm für ein BCM-System bietet die ISO 22301 Möglichkeiten für eine internationale Vergleichbarkeit der Prozesse und Maßnahmen. Durch diese Vergleichbarkeit mit anderen ISO-Normen und dem Aufsetzen auf dem BS25999-2 können durch bereits absolvierte Audits Synergieeffekte erzielt werden.

Vorteilhaft ist zu erwähnen, dass die ISO 22301 ebenfalls einige Punkte des BS25999-1 enthält. Diese waren bisher nicht direkt zertifizierungsrelevant.

Dadurch wurden wesentliche Bereiche, wie bspw. die Managementverantwortung oder Messbarkeit der Maßnahmen und Aktivitäten hervorgehoben und somit unumgänglicher Zertifizierungsbestandteil. Damit kommt die ISO verstärkt der Entwicklung nach, Stakeholder, im Besonderen die Kunden, zentraler in den Fokus der Unternehmensinteressen zu stellen.

Die insgesamt eindeutige und neutrale Anforderungsformulierung ordnet die ISO-Norm nahtlos in die bereits bekannten, weltweit anerkannten Normen anderer Bereiche ein und macht die Anforderungen an ein BCMS transparent und nachvollziehbar.

Für die Unternehmen stellt die Norm im Wesentlichen jene Anforderungen heraus, welche die Organisation und ihre Prozesse für eine Zertifizierung zu erfüllen haben. Für eine konkrete Ausgestaltung oder Umsetzungsunterstützung liefern dagegen eher die beschreibenden Standards bzw. Normen die geeigneten Methoden und Hilfsmittel. Zu diesen zählt neben dem BS25999-1 vor allem auch der vom BSI herausgegebene Standard 100-4 Notfallmanagement.

Die HiSolutions AG unterstützt Sie bei der Umsetzung eines standardkonformen Business Continuity Management Systems und dessen optimale Integration ins Unternehmen und den anderen Management Systemen unter Anwendung dieser Standards bzw. Normen und liefert Ihnen eine individuelle und wirtschaftliche Lösung für Ihre Organisation.

HiSolutions AG - Firmenprofil

Die HiSolutions AG bietet ein umfassendes Portfolio an Dienstleistungen rund um die Themen Governance, Risk und Compliance (GRC). Dabei vereinen wir strategische Beratungskompetenz mit fundierten methodischen Vorgehensweisen und technischer Expertise. Als inhabergeführtes Unternehmen sind wir frei von Marktinteressen Dritter und erbringen unsere Leistungen daher mit größtmöglicher Objektivität. Seit unserer Gründung im Jahr 1994 haben wir unsere Leistungsfelder und die Stärke unseres Teams beständig erweitert.

Die HiSolutions AG ist ein führender deutscher Beratungsdienstleister in den Bereichen Corporate Security, Business Continuity, Information Security und System Security.

Im Geschäftsfeld Business Continuity & Risk Management bietet die HiSolutions AG strategische Beratungslösungen für den Aufbau, die Umsetzung oder die Optimierung organisatorischer, technischer und personeller Maßnahmen in Unternehmen entlang der Wertschöpfungskette an. Diese dienen der Vermeidung oder Minimierung von Ausfällen von zeitkritischen Geschäftsprozessen bzw. zur Steigerung deren Widerstandsfähigkeit.

Das gesamte BCM-Team besteht aus zertifizierten Mitarbeitern (ISO 22301, BS 25999 Lead Auditor) mit langjähriger Erfahrung im Business Continuity & Risk Management von nationalen und internationalen Unternehmen, Organisationen und Regierungen.

Die HiSolutions AG ist als (Mit-)Autorin an den IT-Grundschutzkatalogen und dem BSI-Standard 100-4 Notfallmanagement sowie in mehreren Studien für das BSI und das BMI tätig und sitzt im ISO-Normierungsausschuss zur neuen ISO Standardreihe ISO 223xx Societal Security & Business Continuity. Zudem beteiligt sie sich an größeren Forschungsprojekten im Bereich Krisenmanagement und KRITIS.