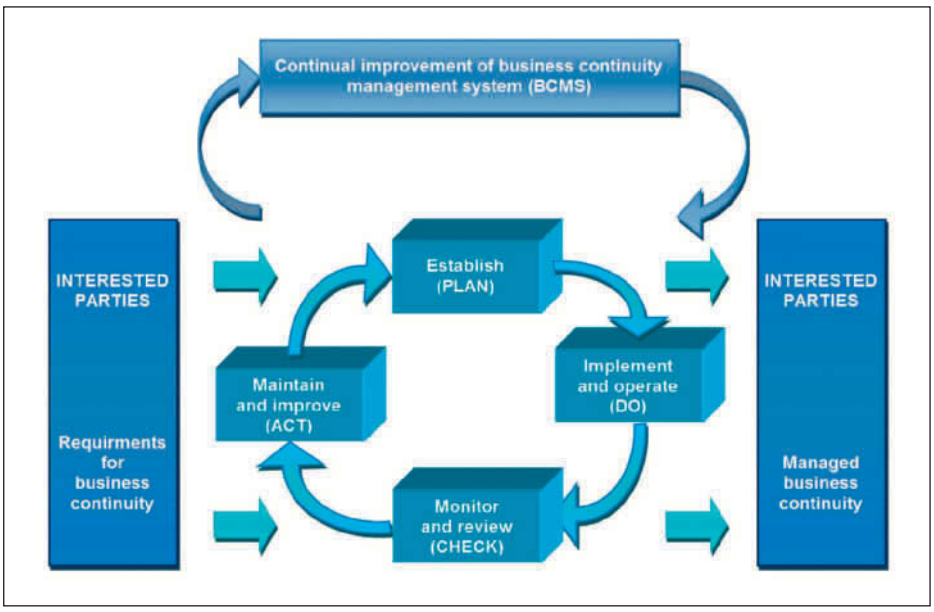
# BCM – der neue ISO-Standard

Der neue ISO-Standard 22301:2012 ist planmässig veröffentlicht worden. Hierbei handelt es sich um den weltweit ersten internationalen Standard für Business Continuity Management (BCM), der Organisationen helfen wird, die Risiken von Betriebsunterbrechungen jeglichen Ursprungs zu reduzieren.

**Von Uwe Müller-Gauss**

Am 15. Juni 2012 wurden von der International Standards Organisation (ISO) die ersten Normen für den Bereich Business Continuity Management veröffentlicht. Es handelt sich dabei um die ISO 22300:2012 Societal Security; Terminology und die ISO 22301:2012 Societal Security; Business Continuity Management Systems; Requirements. Damit wurde ein bedeutender Meilenstein bei der internationalen Harmonisierung von Regelwerken auf diesem Gebiet erreicht. Während die Norm ISO 22300 ein Referenzwerk für die Sprachregelung darstellt, welches die Basis für eine Reihe von Normen des Technical Committee ISO/TC 223 darstellt, wird die ISO 22301 die Nachfolge des bisherigen Referenzstandards BS 25999 antreten. Der internationale Standard ersetzt somit den aktuellen Britischen Standard BS 25999.

Der ISO-Standard 22301 spezifiziert alle Anforderungen, wie ein Kontinuitätsmanagementsystem (engl.: Business Continuity Management; BCM) zu planen, einzurichten, zu realisieren, zu betreiben, zu überwachen, zu überprüfen, zu unterhalten und kontinuierlich zu verbessern ist, um sich wirkungsvoll auf mögliche Betriebsunterbrechungen präventiv vorzubereiten, auf diese zu reagieren oder um sich als Unternehmen von Betriebsunterbrechungen schnellstmög-




**PDCA-Model anhand des BCM-Systems (gem. ISO 22301:2012)**

lich zu erholen. Die in ISO 22301 spezifizierten Anforderungen sind, wie auch in der ISO 31000, allgemein gehalten. Sie sollen auf Organisationen jeglicher Art, ohne Rücksicht auf die Grösse oder Branche, anwendbar sein. Der Umfang der Anwendbarkeit der definierten Anforderungen hängt von der Betriebsumgebung und der Komplexität der Organisation ab.

## Bereiche

Die ISO 22301 ist anwendbar auf Organisationen, welche:

- ein BCM einrichten, implementieren, unterhalten und verbessern möchten
- die Konformität gegenüber Dritten, z.B. Lieferanten, belegen möchten
- eine Zertifizierung ihres Business Continuity Managements durch eine akkreditierte Zertifizierungsstelle anstreben oder eine Konformität mit diesem internationalen Standard selbst deklarieren möchten

## Bausteine zur Umsetzung

Für eine erfolgreiche Umsetzung eines betrieblichen Kontinuitätsmanagements definiert der ISO-Standard – in Anlehnung an das PDCA-Model – eine Reihe von Bausteinen: Ein erstes Modul konzentriert sich auf die Organisation. So ist es wichtig, dass die externen und internen Sachverhalte analysiert werden, die für den Erfolg der Organisation wichtig sind (strategische Erfolgspositionen = SEP) und welche durch eine Betriebsunterbrechung gefährdet werden.

Hierzu gehört beispielsweise die Analyse:

- der Aktivitäten, Aufgaben, Dienstleistungen, Produkte, Partnerschaften, Lieferketten (Supply Chain), sonstigen Stakeholder sowie der potenziellen Auswirkung einer Betriebsunterbrechung
- der Verknüpfungen zwischen der Business-Continuity-Strategie (Policy) und den Unternehmenszielen der Organisation sowie die Abhängigkeit zu anderen Regelwerken
- die Analyse der unternehmensübergreifenden Risikomanagementstrategie
- des Risikoappetits sowie der Risikotragfähigkeit der Organisation
- der Bedürfnisse und Erwartungen von relevanten Stakeholdern
- der Compliance-Anforderungen, d.h. relevanter gesetzlicher, regulatorischer und anderer Anforderungen

## Geltungsbereich

Ebenfalls wird in diesem Teil der Geltungsbereich des betrieblichen Kontinuitätsmanagements bestimmt. Dabei müssen die strategischen Ziele, Schlüsselprodukte und -dienstleistungen, die Risikotoleranz sowie alle regulatorischen und vertraglichen Verpflichtungen oder Verpflichtungen gegenüber Anspruchsberechtigten der Organisation in genügendem Masse berücksichtigt werden.

Im nächsten Modul der ISO 22301 geht es um die Führung. Analog zum betrieblichen Risikomanagement ist eine Vorbildfunktion des Topmanagements (Commitment) entscheidend für eine erfolgreiche Umsetzung. Das Topmanagement muss die Relevanz und Verpflichtung eines BCM fortlaufend demonstrieren. Durch Führung kann das Management eine Risikokultur schaffen, sodass alle Akteure bzw. Mitarbeiter in dem Prozess involviert sind.

Das Management ist verantwortlich:

- sicherzustellen, dass das BCM kompatibel mit der strategischen Ausrichtung der Organisation ist
- die BCM-Anforderungen in die Geschäftsprozesse der Organisation zu integrieren
- die notwendigen Ressourcen für das BCM bereitzustellen
- die Bedeutung eines wirksamen BCM zu kommunizieren
- sicherzustellen, dass das BCM die erwarteten Ergebnisse erzielt
- die kontinuierliche Verbesserung (Continuous Improvement Process, CIP) des BCM zu ermöglichen
- eine Business-Continuity-Strategie (Überlebensgarantie) zu erstellen und zu kommunizieren
- sicherzustellen, dass die BCM-Ziele durch die Festlegung von kritischen Prozessen und Wiederanlaufprioritäten sowie geeigneter Notfallpläne (BCP) erreicht werden
- sicherzustellen, dass klare Verantwortlichkeiten und Befugnisse zugeordnet werden

Unter kontinuierlicher Verbesserung (KVP; engl.: Continuous Improvement Process, CIP) werden alle Massnahmen zusammengefasst, die in der ganzen Organisation getroffen werden, um die Wirksamkeit (Erreichung der Ziele) und Effizienz (ein optimales Kosten-/Nutzen-Verhältnis) zu erhöhen.

In einem nächsten Modul geht es um die Planung des betrieblichen Kontinui-


**BCM-Lebenszyklus gemäss Good Practice Guidelines**

tätsmanagements. Diese Phase wird als kritisch eingestuft, da die Definition der strategischen Ziele und Leitprinzipien das Fundament für das BCM bildet. Die Business-Continuity-Ziele müssen u.a.:

- konsistent sein mit der Business-Continuity-Strategie (Policy)
- messbar sein
- anwendbare Anforderungen beachten
- überwacht und gegebenenfalls aktualisiert werden

## Ressourcen

Der nächste Baustein beschäftigt sich mit der Unterstützung des BCM durch adäquate Ressourcen. Das nachhaltige Management eines wirksamen BCM basiert auf einem soliden Fundament angemessener Ressourcen. Diese beinhalten u.a. qualifiziertes Personal, unterstützende Dienstleistungen, ein gelebtes Risikobewusstsein sowie eine zeitgemässe Kommunikation. In diesem Kontext spielt vor allem die interne wie auch die externe Kommunikation eine grosse Rolle. Auch die Anforderungen an die Erstellung, die Aktualisierung und die Kontrolle der BCM-Dokumentation sind Bestandteil dieses Moduls.

Nach der Planung des betrieblichen Kontinuitätsmanagements muss eine Organisation das BCM-System aufbauen und in Betrieb nehmen. Dazu haben sich die folgenden Module bewährt:

**Business Impact Analysis (BIA):** Hierbei handelt es sich um eine Methode zur Sammlung und Identifizierung von kritischen Prozessen und Funktionen innerhalb einer Organisation (siehe Impact-Kriterien im Kasten), um die den Prozessen zugrunde liegenden Ressourcen zu erfassen. Des Weiteren können durch eine BIA wechselseitige Abhängigkeiten zwischen Prozessen resp. Unternehmensbereichen aufgezeigt, die Auswirkungen bei Ausfällen von Prozessen, die Kritikalität jedes Prozesses und die benötigte Wiederanlaufzeit aufgedeckt werden.

**Risikobeurteilung (RA):** Die ISO 22301 referenziert auf den internationalen Risikomanagement-Standard ISO 31000. Die ISO 31000 weist drei spezifische Merkmale auf: Es handelt sich erstens um einen umfassenden Top-down-Ansatz, zweitens wird Risikomanagement als Führungsaufgabe dargestellt und drittens handelt es sich um eine allgemein gehaltene Basis-Norm.

**Business-Continuity-Strategie (BCS):** Nachdem die Anforderungen über die BIA und die Risikobeurteilung erfasst worden sind, müssen Überlebensstrategien entwickelt werden, um Massnahmen zu identifizieren, welche es der Organisation erlauben, auf der Basis ihrer Risikotoleranz sowie Risikotragfähigkeit und innerhalb festgelegter Ziele für die Wiederherstellungszeit kritische Prozesse zu schützen resp. wiederherzustellen. Dabei ist die BCM-Strategie auf die gesamte Geschäftsstrategie auszurichten und ist als ein integraler Bestandteil der Unternehmensstrategie zu verstehen.

**Business-Continuity-Verfahren (BCP):** Die Organisation muss Verfahren dokumentieren, um die Kontinuität von Aktivitäten und das Management von Betriebsunterbrechungen sicherzustellen. Diese Verfahren müssen:

- einen angemessenen Plan für die interne und externe Kommunikation festlegen
- flexibel sein, um auf unerwartete Bedrohungen und sich verändernde interne und externe Bedingungen antworten zu können
- spezifisch sein hinsichtlich der konkreten Schritte, die anlässlich einer Betriebsunterbrechung zu erfolgen haben
- auf Auswirkungen von Ereignissen fokussieren, die möglicherweise den Betrieb unterbrechen könnten
- entwickelt werden auf der Basis der Analyse von Wechselwirkungen und
- wirksam sein bei der Minimierung von Folgen durch die Implementierung von angemessenen Strategien zur Schadensminderung

**Üben und Testen:** Um sicherzustellen, dass die Business-Continuity-Pläne (BCP = Notfallpläne) mit den Business-Continuity-Zielen konsistent sind, hat die Organisation sie regelmässig zu testen. Üben und Testen sind die Prozesse zur Bestätigung von Business-Continuity-Plänen, um zu gewährleisten, dass die gewählten Strategien sicherstellen, innerhalb der durch das Management bestimmten Zeitfenster Antworten und Wiederherstellungsergebnisse zu liefern, und so das Überleben der Organisation garantieren.

**Pflege:** Sobald das BCM-System implementiert ist, ist das System ständig zu überwachen und periodisch zu überprüfen, um seinen Betrieb laufend zu verbessern/zu optimieren:

- Messen der Leistung von Prozessen, Verfahren und Funktionen, die kritische Prozesse schützen
- Überwachung der Übereinstimmung mit dem Standard und den Business-Continuity-Zielen
- Überwachung der historischen Erfahrungen einer mangelhaften Leistung des betrieblichen Kontinuitätsmanagements
- Ausführung von regelmässigen internen Audits

## FAZIT: «ALTER WEIN IN NEUEN SCHLÄUCHEN»

Der neue ISO-Standard 22301 ist auf der Basis der BS 25999 entwickelt worden, was allen bisherigen Anwendern der Good Practice Guidelines (GPG siehe Abbildung 2) von BCI die Gewissheit gibt, auch in Zukunft mit den neuen ISO-Standards konform zu sein. ■

UWE MÜLLER-GAUSS
ist geschäftsführender Inhaber der auf Sicherheit, Risiko-, Krisen- und Kontinuitätsmanagement spezialisierten MÜLLER-GAUSS CONSULTING in Hinwil. Über 20 Jahre Erfahrung bei der Realisierung von Security- & Risk-Management-Strategien, Notfall- und Evakuierungsorganisationen und Führungsinstrumente für das Kontinuitätsmanagement (BCM).

**Knowing.** **Not guessing.**

# 20 Jahre Erfahrung in den Bereichen

## PRÄVENTION - RESILIENCE

Bauherrenberatung/ Projektmanagement
Sicherheitsplanung/ Trouble-Shooting
Integrale Tests/ Security & Risk Audits/ Reviews
Risikoanalysen/ Risikomanagement Systeme

## EREIGNISBEWÄLTIGUNG - BCM

Business Impact Analysen/ Überlebensstrategien
Business Continuity Management Manuals
Notfall- und Evakuierungskonzepte/ Notfallpläne
Krisenmanagement Handbücher
Krisenstabs- und Evakuierungsübungen

**Es ist besser, beizeiten Dämme zu bauen,
als auf die Vernunft der Flut zu hoffen!**

MÜLLER
GAUSS
CONSULTING

**MÜLLER-GAUSS CONSULTING**
Security | Risk | Crisis | Continuity Management

+41 44 938 05 04 ● uwe.mueller@gauss-consulting.ch ● www.gauss-consulting.ch