

Business Continuity Plan (BCP): Unternehmen resilient gegen Ausfälle absichern

Ein Business Continuity Plan (BCP) ist ein dokumentierter Notfallplan, der sicherstellt, dass ein Unternehmen kritische Prozesse bei Störungen, Ausfällen oder Lieferunterbrechungen aufrechterhalten oder zeitnah wiederherstellen kann. Im Einkauf und in der Lieferkette richtet sich der Plan häufig auf Lieferantenausfälle, Rohstoffengpässe und Produktionsstillstände. Für technische Einkäufer ist der BCP ein zentrales Instrument, um Versorgungssicherheit systematisch statt spontan zu organisieren. Er wirkt damit nicht nur als Krisenreaktion, sondern auch als Element einer belastbaren Beschaffungsstrategie.

Das Wichtigste in Kürze

- Ein BCP legt fest, welche Prozesse kritisch sind, welche Ausfallzeiten tolerierbar sind und wie der Betrieb im Störfall aufrechterhalten wird.
- Im Einkauf fokussiert der Plan typischerweise auf Lieferantenausfälle, Ersatzquellen, Sicherheitsbestände und Notfalllogistik.
- Kennzahlen wie Recovery Time Objective und Recovery Point Objective machen die Wiederaufnahmezeiten messbar.
- Ein wirksamer BCP wird regelmäßig getestet, z. B. durch Szenariodurchspiele und Störungssimulationen.
- Der Plan sollte eng mit dem Lieferantenmanagement verzahnt sein, etwa über Lieferantenselbstauskunft und das Lieferantenratingmodell.
- Ohne Aktualisierung veralten BCPs schnell; üblich ist eine jährliche Prüfung sowie eine Revision nach jedem realen Störfall.

Definition: Business Continuity Plan (BCP)

Der Business Continuity Plan ist ein strukturierter Handlungsplan, der beschreibt, wie ein Unternehmen kritische Geschäfts- und Lieferprozesse bei Zwischenfällen fortführt oder schnell wiederherstellt. Er konkretisiert die Business Continuity Management (BCM)-Strategie auf operativer Ebene. Im Einkauf steht dabei die Versorgungssicherheit von Material, Bauteilen und Dienstleistungen im Mittelpunkt.

Abgrenzung zu Risikomanagement und BCM

Risikomanagement identifiziert und bewertet Gefährdungen frühzeitig, das übergeordnete BCM legt Ziele und Verantwortlichkeiten fest. Der BCP übersetzt beides in konkrete Maßnahmen: Wer handelt wie, mit welchen Ressourcen und bis wann? Im Einkauf ergänzt der BCP das Marktmodell und die Marktbeobachtung um einen aktiven Ausfallplan statt reiner Risikoübersicht.

Typische Auslöser für einen BCP im Einkauf

Praxisnahe Auslöser sind Lieferantenausfälle, Insolvenzen, Rohstoffknappheit, Naturkatastrophen, Logistikstörungen oder IT-Ausfälle wie der Wegfall kritischer Systeme der Bestellhistorie und Beschaffungsdaten. Auch gezielte Anforderungen von Kunden, etwa in der Leistungsbeschreibung von OEM-Vergaben, fordern häufig einen dokumentierten BCP beim Zulieferer. Häufig gehen solche Anforderungen mit Bewertungskriterien einher, die im Zuliefereraudit geprüft werden.

Methoden und Vorgehen: BCP im Einkauf aufbauen

Ein wirksamer BCP folgt einem methodischen Ablauf: kritische Prozesse und Teile identifizieren, Risiken bewerten, Maßnahmen definieren und den Plan regelmäßig testen. Für Einkäufer bedeutet das vor allem, die Versorgung kritischer Artikel und Zulieferer systematisch abzubilden.

Kritikalitätsanalyse und Ausfallrisiko bewerten

Zunächst werden Teile, Zulieferer und Prozesse danach bewertet, wie stark ein Ausfall Produktion und Umsatz trifft. Typische Kriterien sind Lieferzeiträume, Ersatzquellenverfügbarkeit, Alleinlieferantenanteil und der Einfluss auf die Kapazitätsplanung. Häufig nutzt man Portfolioansätze: Hohe Kritikalität und hohes Lieferrisiko führen zu intensiven Maßnahmen, niedrige Werte zu Standardprozessen. Die Ergebnisse fließen in das Lieferantenratingmodell und in die laufende Marktbeobachtung ein.

Second Source, Sicherheitsbestand und Notfalllogistik

Kernmaßnahmen sind Zweitquellen, vereinbarte Sicherheitsbestände, vertragliche Lieferzusagen sowie dokumentierte Notfallrouten für Transport und Zoll. In der Praxis liegt der Sicherheitsbestand für kritische Artikel häufig bei zwei bis acht Wochen Bedarf, abhängig von Wiederaufnahmezeit und Lagernutzen. Beim Aufbau von Zweitquellen ist eine saubere Leistungsbeschreibung wichtig, damit Ersatzlieferanten technische Anforderungen und Prüfprozesse eindeutig erfüllen.

Lieferantenseitige BCP-Anforderungen und Verträge

Einkäufer fordern von kritischen Zulieferern einen eigenen BCP, häufig über die Lieferantenselbstauskunft oder ein Zuliefereraudit. Vertraglich können sich Verpflichtungen zu Alternativfabriken, Warnzeiten bei Störungen und Prioritätszusagen ergeben. Auch Preismechanismen wie ein Raw Material Surcharge lassen sich so mit Ausfallszenarien verknüpfen, damit Preisanpassungen bei Rohstoffengpässen nicht zur ungeplanten Kostenfalle werden.

Wichtige KPIs für den Business Continuity Plan

Ein BCP wirkt nur, wenn Fortschritte und Bereitschaft messbar sind. Die folgenden Kennzahlen haben sich in der Praxis als sinnvolle Orientierung etabliert; konkrete Zielwerte hängen von Branche und Kritikalität ab.

Zeit- und Datenziele: RTO und RPO

Die Recovery Time Objective (RTO) gibt an, innerhalb welcher Zeit ein Prozess oder eine Lieferung nach Ausfall wieder laufen soll. Die Recovery Point Objective (RPO) definiert, wie viele Daten oder Aufträge maximal verloren gehen dürfen. Im Einkauf kommen daraus konkrete Anforderungen: Sicherheitsbestand, Zweitquellenverfügbarkeit und Notfalllogistik müssen diese Ziele realistisch hergeben.

Versorgungs- und Testquoten

Weitere praktikable Kennzahlen sind der Anteil kritischer Teile mit dokumentierter Zweitquelle, der Anteil getesteter BCP-Szenarien pro Jahr sowie die Lieferantenabdeckung mit gültiger Lieferantenselbstauskunft und aktualisierter BCP-Zusage. Ergänzend lässt sich die durchschnittliche Wiederaufnahmezeit nach realen Störfällen als Lernkennzahl heranziehen. Auch die Cash-to-Cash Cycle-Dauer reagiert auf Ausfälle, wenn Notkäufe zu längeren Zahlungs- und Vorfinanzierungszeiträumen führen.

Risiken und Kontrollen: typische Fehlerquellen und Gegenmaßnahmen

BCPs scheitern in der Praxis häufig nicht am fehlenden Plan, sondern an mangelnder Pflege, unrealistischen Annahmen oder fehlender Abstimmung mit Lieferanten und Logistik. Kontrollen und klare Verantwortlichkeiten wirken dem entgegen.

Planverfall und fehlende Tests

Ein BCP, der nur im Schrank liegt, veraltet schnell: Kontaktdaten, Kapazitäten und Ersatzquellen ändern sich. Kontrollinstrumente sind jährliche Reviews, geplante Testszenarien und die Pflicht zur Planrevision nach jedem realen Störfall. Sinnvoll ist die Verankerung in der Lieferantenstammdatenpflege, damit BCP-Zusagen, Ansprechpartner und Alternativstandorte aktuell bleiben.

Vertragslücken und Kostenkontrolle im Störfall

Häufig fehlen vertragliche Verpflichtungen zu Ersatzkapazitäten oder Warnzeiten. Auch Kostenaspekte werden übersehen: Notkäufe, Luftfracht oder Zusatzschichten treiben Prozesskosten und können über abweichende Zahlungsziele die Cashflow-Wirkung von Zahlungszielen verschlechtern. Hilfreich sind vorab definierte Abweichgenehmigungen und ein klarer Preisabweichungsworkflow, damit Notfallentscheidungen schnell, aber kontrolliert getroffen werden.

Abhängigkeiten von Alleinlieferanten und Ressourcen

Alleinlieferanten sind häufig wirtschaftlich attraktiv, erhöhen aber das Ausfallrisiko erheblich. Gegenmaßnahmen sind Zweitquellen für kritische Teile, vertragliche Kapazitätsreserven oder strategische Lager. Bei Preisverhandlungen können Alternativquellen auch als Verhandlungshebel wirken; zusätzliche Erkenntnisse liefert ein Energieaudit Lieferant, wenn Energieknappheit oder -preise den Standort des Zulieferers destabilisieren könnten.

Aktuelle Entwicklungen: Lieferkette, Digitalisierung und Nachhaltigkeit

Anforderungen an Business Continuity steigen: Komplexere Lieferketten, geopolitische Risiken, Energiepreisschwankungen und neue regulatorische Pflichten erhöhen den Druck auf dokumentierte Ausfallvorsorge. Digitalisierung hilft, den Plan aktuell und einsatzfähig zu halten.

Regulatorische Anforderungen und Lieferkettendue-Diligence

Gesetze zu Lieferkettensorgfalt, Berichtspflichten und Produktsicherheit verlangen zunehmend transparente Lieferketten. Ein BCP kann diese Transparenz aufgreifen, da beide Themen Lieferantenrisiken und Ersatzquellen systematisch erfassen. Wichtig ist die Einhaltung regulatorischer

Pflichten wie dem Verpackungsgesetz (VerpackG) bei der Notfalllogistik; konkrete rechtliche Bewertungen sollten im Einzelfall mit Fachleuten geprüft werden.

Datenkontrolle, Systeme und digitale Frühwarnindikatoren

Digitale Tools erleichtern die laufende Überwachung von Lieferterminen, Kapazitäten und Marktindikatoren. Voraussetzung ist eine saubere Datenkontrolle: Wer darf Risiko- und BCP-Daten sehen, wie werden Lieferanteninformationen geschützt? Auch die Katalogverwaltung für kritische Artikel profitiert, weil Ersatzquellen und Freigabestatus schneller auffindbar sind. Frühwarnsignale aus Marktbeobachtung und Lieferantenkommunikation lassen sich so systematisch in den BCP einspeisen.

Typische Kennzahlen

Recovery Time Objective (RTO): je nach Kritikalität

Zielzeit für die Wiederherstellung eines Prozesses nach Ausfall, z. B. Stunden bis Wochen

Anteil kritischer Teile mit Zweitquelle: typischerweise > 80 %

Anteil der als kritisch eingestuften Artikel mit dokumentierter Ersatzquelle

Getestete BCP-Szenarien pro Jahr: häufig 1–2 Szenarien

Anzahl durchgeführter Tests oder Tabletop-Übungen pro Jahr

Durchschnittliche Wiederaufnahmezeit nach Störfall: Richtwert abhängig von Branche

Tatsächlich benötigte Zeit bis zur Wiederherstellung der Versorgung, Vergleich gegen RTO

Praxisbeispiel

Ein mittelständischer Maschinenbauer mit rund 400 Mitarbeitern erlitt nach einem Brand bei seinem Alleinlieferanten für gehäuste Gussbauteile einen Produktionsstillstand von mehreren Wochen. In der Folge baute das Unternehmen einen strukturierten BCP für die kritischen A-Teile auf.

- Einstufung aller Teile nach Kritikalität und Lieferausfallrisiko, Start mit rund 60 kritischen Artikeln
- Aufbau von Zweitquellen mit sauberer Leistungsbeschreibung und Prüfprozess für drei Gussbauteile-Familien
- Vereinbarung von Sicherheitsbeständen von typischerweise vier Wochen Bedarf sowie Warnpflichten im Liefervertrag
- Jährliches BCP-Tabletop-Szenario mit Vertrieb, Einkauf und Logistik inklusive Dokumentation der Ergebnisse

Fazit

Ein Business Continuity Plan verwandelt Liefer- und Produktionsrisiken in einen geordneten Handlungsablauf. Für den technischen Einkauf ist er kein isoliertes Sicherheitspapier, sondern verzahnt sich mit Lieferantenauswahl, Vertragsdesign, Beständen und Kapazitätsplanung. Entscheidend sind messbare Ziele wie RTO und RPO, regelmäßige Tests und aktuelle Lieferantendaten. Wer kritische Artikel systematisch absichert, reduziert Stillstände, Notkaufkosten und Verhandlungsnachteile. Ein gepflegter BCP wird damit zum sichtbaren Qualitätsmerkmal gegenüber Kunden und Prüfern.

Häufige Fragen

Was ist ein Business Continuity Plan einfach erklärt?

Ein Business Continuity Plan ist ein Notfallplan, der beschreibt, wie ein Unternehmen bei Ausfällen oder Störungen wichtige Prozesse weiterführt oder schnell wiederherstellt. Er legt Verantwortlichkeiten, Ersatzlösungen und Wiederanlaufzeiten fest. Im Einkauf sichert er vor allem die Versorgung mit kritischen Materialien und Zulieferleistungen ab.

Was gehört in einen Business Continuity Plan?

Typische Bestandteile sind eine Liste kritischer Prozesse und Artikel, Risikobewertungen, Maßnahmen wie Zweitquellen und Sicherheitsbestände, Kontaktdaten, Wiederanlaufzeiten (RTO/RPO) sowie Kommunikationswege im Störfall. Wichtig sind außerdem Test- und Aktualisierungsregeln. Im Einkauf gehört auch die Verzahnung mit Lieferverträgen und Lieferantenanforderungen dazu.

Wie oft sollte ein BCP überprüft werden?

In der Praxis hat sich eine jährliche Prüfung bewährt. Zusätzlich sollte der Plan nach jedem realen Störfall, nach wesentlichen Lieferantenwechseln oder nach Organisationsänderungen aktualisiert werden. Geplante Testszenarien zeigen, ob Annahmen zu Beständen, Kapazitäten und Wiederaufnahmezeiten noch stimmen.

Was ist der Unterschied zwischen BCP und Disaster Recovery?

Disaster Recovery bezieht sich meist auf die Wiederherstellung von IT-Systemen und Daten nach einem Ausfall. Der Business Continuity Plan ist breiter angelegt und umfasst alle kritischen Geschäftsprozesse, also auch Produktion, Logistik und Beschaffung. Disaster Recovery kann daher als Teilbereich des BCP verstanden werden.

Wie implementiert man einen BCP im Einkauf?

Zunächst werden kritische Teile und Lieferanten identifiziert und nach Ausfallrisiko bewertet. Darauf aufbauend definiert man Maßnahmen wie Zweitquellen, Sicherheitsbestände, vertragliche Warnpflichten und Notfalllogistik. Abschließend werden Verantwortliche benannt, KPIs wie RTO festgelegt und der Plan regelmäßig getestet.

Welche Rolle spielt der BCP bei Zulieferern und Audits?

Viele OEMs und große Abnehmer erwarten von ihren Zulieferern einen dokumentierten BCP, oft geprüft über Lieferantenselbstauskunft oder Audits. Ein nachweisbarer Plan verbessert damit die Position im Lieferantenrating. Zulieferer sollten ihren BCP an Kundenanforderungen anpassen und relevante Nachweise bereithalten.