ISO 22301
Checkliste zur Selbsteinschätzung

Wie bereit sind Sie?

Dieses Dokument wurde erstellt, um die Bereitschaft Ihres Unternehmens für eine ISO 22301 Business Continuity Management System-Zertifizierung zu beurteilen. Das Ausfüllen dieses Fragebogens ermöglicht Ihnen eine Selbsteinschätzung Ihrer Organisation und zeigt Ihnen, wo Sie in Bezug auf die Hauptanforderungen der Norm stehen.

Kontext des Unternehmens

Haben Sie die externen und internen **Aspekte** ermittelt, die für den Zweck Ihres Unternehmen relevant sind und Ihre Leistungsfähigkeit beeinträchtigen, um die angestrebten Ergebnisse Ihres Business-Continuity-Management-Systems (BCMS) zu erreichen?

Haben Sie die Möglichkeit, Änderungen an Problemen regelmäßig zu überprüfen und zu überwachen?

Haben Sie die Bedürfnisse und Erwartungen der Interessengruppen ermittelt, die für das BCMS relevant sind, und überprüfen Sie diese regelmäßig?

Haben Sie den Umfang Ihres BCMS festgelegt und haben Sie dabei die externen und internen Fragen, der beteiligten Gruppen und der von anderen Unternehmen durchgeführten Aktivitäten berücksichtigt?

Kennen Sie die Anforderungen von Interessengruppen, einschließlich behördlicher und gesetzlicher Vorschriften sowie die Ihrer Kunden?

Sind die mit Fragen und Anforderungen verbundenen Risiken und Chancen berücksichtigt worden?

Wurde eine kontinuierliche Verbesserung in Betracht gezogen?

Führung

Hat die Geschäftsleitung die Verantwortung für die Wirksamkeit des BCMS übernommen und hat sie die Bedeutung eines wirksamen BCMS vermittelt?

Sind die Unternehmenspolitik und -ziele für d**as** BCMS, die mit dem Kontext und der strategischen Ausrichtung des Unternehmens vereinbart sind, festgelegt und kommuniziert worden?

Tragen die Funktionen die Autorität für die Gewährleistung der Konformität und Berichterstattung sowie die Verantwortung?

Wurde ein Programm entwickelt und eingeführt, das sicherstellt, dass der BCMS seine Ergebnisse, Anforderungen und Ziele erreicht?

Fortsetzung >>

Planung

Sind die Risiken und Chancen, die angegangen werden müssen, um sicherzustellen, dass der BCMS sein/ihr angestrebtes/e Ergebnis/e erreichen kann, festgelegt worden?

Hat das Unternehmen Maßnahmen zur Bewältigung dieser Risiken und Chancen geplant und in die Systemprozesse integriert?

Wurden messbare Ziele für die Geschäftskontinuität festgelegt, dokumentiert und im gesamten Unternehmen mit einem Plan zur Erreichung dieser kommuniziert?

Unterstützung

Stellt das Unternehmen, Ressourcen die für die Einrichtung, Implementierung, Aufrechterhaltung und kontinuierliche Verbesserung des BCMS benötigt werden (einschließlich der Menschen, der Infrastruktur und der Umgebung für den Betrieb der Prozesse) zur Verfügung?

Wird dieser Prozess von den Mitarbeitern in den definierten BCMS-Rollen eingehalten?

Hat das Unternehmen das benötigte Wissen, das für die Personen, die die Aufgaben des BCMS übernimmt, festgelegt?

Hat das Unternehmen sichergestellt, dass die Personen, die die Leistung und Wirksamkeit des BCMS beeinflussen können, auf der Grundlage einer geeigneten Ausbildung oder Erfahrung kompetent sind oder hat sie Maßnahmen ergriffen, dass diese Personen die erforderliche Kompetenz erwerben können?

Sind die erforderlich dokumentierten Informationen des Standards festgehalten, die für eine Implementierung des ISMS benötigt wird?

Werden die dokumentierten Informationen kontrolliert in einer angemessen Art und Weise geschützt, verteilt, gespeichert und aufbewahrt? Werden Änderungskontrollen einschließlich der vom Unternehmen für den BCMS benötigten Dokumente externen Ursprungs durchgeführt?

Betrieb

Haben Sie ein Programm ausgearbeitet und umgesetzt, um sicherzustellen, dass der BCMS seine Ziele erreicht?

Gibt es einen Plan, um die Notwendigkeit von Änderungen am ISMS und BCMS festzustellen und deren Umsetzung zu verwalten?

Wenn Änderungen geplant sind, werden sie kontrolliert durchgeführt und die Maßnahmen festgehalten, die ergriffen werden, um nachteilige Folgen zu mildern?

Wenn Sie Prozesse ausgelagert haben, werden diese angemessen kontrolliert?

Gibt es einen formalen und dokumentierten Prozess zum Verständnis des Unternehmens durch eine Business-Impact-Analyse (BIA)?

Gibt es einen formellen Prozess zur Bestimmung von Kontinuitätszielen auf der Grundlage des Verständnisses der Auswirkungen von Zwischenfällen?

Ermöglicht die BIA eine Priorisierung der Zeitrahmen für die Wiederaufnahme jeder Aktivität (Recovery Time Objectives) und verfügt sie über Mindestniveaus für die Wiederaufnahme der identifizierten Aktivitäten?

Sind diese Maßnahmen dokumentiert worden?

Basiert die BC-Strategie auf den Ergebnissen der BIA und der Risikobewertung?

Schützt die BC-Strategie die priorisierten Aktivitäten und sorgt für eine angemessene Kontinuität und Wiederherstellung dieser, derene Abhängigkeiten und Ressourcen?

Bietet die BC-Strategie die Möglichkeit, Auswirkungen zu mildern, auf sie zu reagieren und sie zu bewältigen?

Sind priorisierte Zeitrahmen für die Wiederaufnahme aller Aktivitäten festgelegt worden?

Wurden die BC-Fähigkeiten der Lieferanten bewertet und eingedämmt?

Wurde der Ressourcenbedarf für die ausgewählten Strategieoptionen festgelegt, einschließlich Personen, Informationen und Daten, Infrastruktur, Einrichtungen, Verbrauchsmaterialien, IT, Transport, Finanzen und Partner-/Lieferantenleistungen?

Sind Maßnahmen zur Reduzierung der Wahrscheinlichkeit, Dauer oder die Auswirkungen einer Störung für identifizierte Risiken berücksichtigt und umgesetzt worden? Stehen diese im Einklang mit der Risikobereitschaft des Unternehmens?

Wurden dokumentierte BC-Verfahren eingeführt, um einen Zwischenfall zu bewältigen? Wurden in der BIA, Kontinuitätsaktivitäten auf der Grundlage von Wiederherstellungszielen festgelegt?

Sind interne und externe Kommunikationsprotokolle als Teil dieser Verfahren eingerichtet worden?

Gibt es eine Struktur (Incident Response Structure, IRS), die die Reaktion des Managements und Personals auf einen Zwischenfall, detailliert beschreibt?

Umfassen die IRS und die damit verbundenen Verfahren Schwellenwerte, Bewertung, Aktivierung, Ressourcenbereitstellung und Kommunikation?

Verfügen die Mitarbeiter in Ihrer IRS über die notwendigen Kompetenzen, um ihre Aufgaben zu erfüllen? Werden diese dokumentiert, um dies zu belegen?

Gibt es ein Verfahren zur Erkennung und Überwachung von Vorfällen, das die Aufzeichnung wichtiger Informationen, getroffener Maßnahmen und Entscheidungen einschließt?

Fortsetzung >>

Betrieb – *Fortsetzung*

Gibt es ein Verfahren zur Verwaltung interner und externe Kommunikation während eines störenden Zwischenfalls?

Gibt es ein Verfahren für den Erhalt und die Reaktion auf Warnungen von externen Agenturen und Notfallhelfern?

Gibt es ein Verfahren für die Herausgabe von Alarm- und Warnmeldungen? Wird diese Kommunikation regelmäßig geübt und die Ergebnisse dokumentiert?

Gibt es dokumentierte Pläne/Verfahren zur Wiederherstellung des Geschäftsbetriebs nach einem Vorfall, spiegeln sie die Bedürfnisse derer, die sie nutzen und alle wesentlichen Informationen, die sie benötigen?

Definieren die Pläne Rollen und Verantwortlichkeiten und einen Prozess zur Aktivierung der Reaktion?

Berücksichtigen die Pläne die Bewältigung der unmittelbaren Folgen einer Unterbrechung, insbesondere das Wohlergehen von Personen, Optionen für die Reaktion und weitere Schadensvermeidungen?

Beschreiben die Pläne im Einzelnen, wie man mit Interessengruppen kommuniziert (einschließlich der Medien) während der Unterbrechung und wie man Prioritäten für Aktivitäten setzt?

Enthalten die Pläne ein Verfahren für die Rücknahme von Stellungnahmen und die Rückkehr zum normalen Betrieb?

Sind die Business-Continuity-Verfahren in geplanten Abständen und mit geeigneten Szenarien getestet worden, um sicherzustellen, dass sie mit Ihren BC-Zielen übereinstimmen?

Wurden für die Tests nach der Übung formelle Berichte erstellt und die Ergebnisse überprüft, um sicherzustellen, dass sie zu Verbesserungen führen?

Bewertung der Leistung

Haben Sie festgelegt, was überwacht und gemessen werden muss, wann, von wem, mit welchen Methoden und wann die Ergebnisse ausgewertet werden sollen?

Werden die Ergebnisse der Überwachung und Messung dokumentiert?

Werden periodisch interne Audits durchgeführt, um zu überprüfen, ob das BCMS wirksam ist und sowohl den Anforderungen der ISO 22301:2019 als auch des Unternehmens entsprechen?

Hat die Organisation ein Programm für interne Audits des BCMS eingerichtet?

Werden die Ergebnisse dieser Audits der Leitung mitgeteilt, dokumentiert und aufbewahrt?

Hat das Unternehmen in den Fällen, in denen Nichtkonformitäten festgestellt werden, geeignete Prozesse für die Verwaltung von Nichtkonformitäten und die damit verbundenen Korrekturen eingerichtet?

Nimmt die Geschäftsleitung regelmäßige und periodische Überprüfungen des BCMS vor?

Hat das Ergebnis der BCMS-Management-Prüfung, Änderungen und Verbesserungen ermittelt?

Werden die Ergebnisse der Management-Bewertung dokumentiert, umgesetzt und gegebenenfalls an die Interessengruppen weitergeleitet?

Wenn Nichtkonformitäten festgestellt werden, hat das Unternehmen geeignete Prozesse für das Verwalten von Nichtkonformitäten und die damit verbundenen Korrekturmaßnahmen eingeführt?

Verbesserung

Wurden Maßnahmen zur Kontrolle, Korrektur und Bewältigung der Folgen von Nichtkonformitäten identifiziert?

Wurde der Handlungsbedarf zur Beseitigung der Grundursache von Nichtkonformitäten evaluiert, um ein erneutes Auftreten zu verhindern?

Sind identifizierte Maßnahmen umgesetzt und auf ihre Wirksamkeit überprüft worden und haben zu Verbesserungen des BCMS geführt?

Werden dokumentierte Informationen als Beweis für die Art der Nichtkonformitäten, die ergriffenen Maßnahmen und die Ergebnisse aufbewahrt?

Erfahren Sie mehr
Tel.: +49 69 2222 8 9200
Website: bsigroup.de

BSI/UK/852/SC/0516/EN/BLD