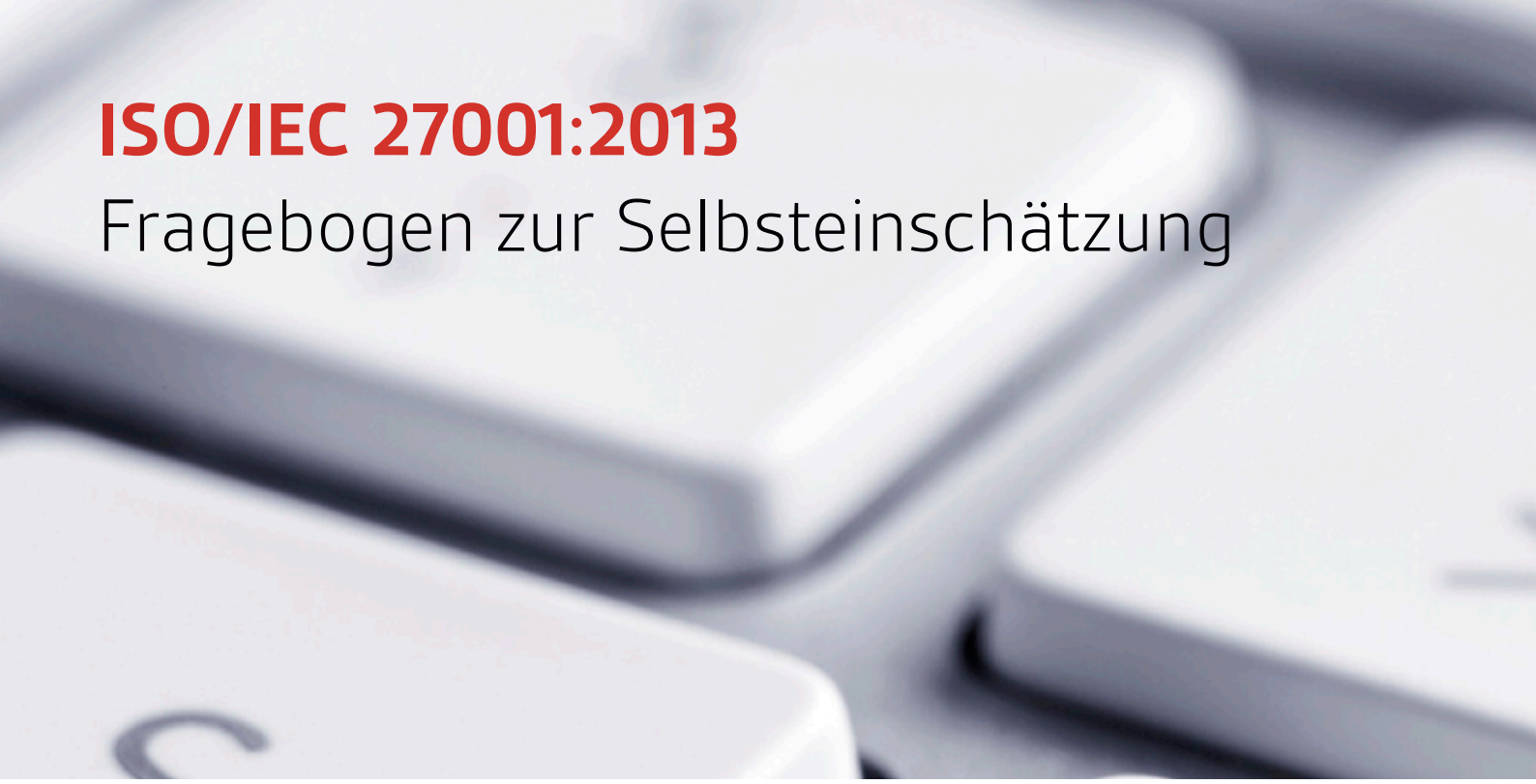

ISO/IEC 27001:2013

Fragebogen zur Selbsteinschätzung

Wie bereit sind Sie?

Dieses Dokument wurde entwickelt, damit Sie überprüfen können, ob Ihr Unternehmen für eine Zertifizierung gemäß ISO/IEC 27001:2013 Informationssicherheitsmanagement bereit ist. Die Ergebnisse dieses Fragebogens ermöglichen es Ihnen, Ihr Unternehmen selbst einschätzen zu können und herauszufinden, wie der aktuelle Stand bei der Erfüllung der Hauptanforderungen der Norm ist.

Kontext der Organisation

- Haben Sie die externen und internen Faktoren bestimmt, die für den Zweck Ihres Unternehmens relevant sind und die einen Einfluss auf Ihre Fähigkeit haben, die gewünschten Ergebnisse Ihres Informationssicherheits-managementsystems (ISMS) zu erzielen?
- Verfügen Sie über ein System zur regelmäßigen Revision und Überwachung von Änderungen dieser Faktoren?
- Haben Sie die Bedürfnisse und Erwartungen der beteiligten Parteien bestimmt, die für das ISMS relevant sind, und überprüfen Sie diese regelmäßig?
- Haben Sie den Anwendungsbereich Ihres ISMS bestimmt und wurden dabei externe und interne Faktoren, beteiligte Parteien und alle Aktivitäten, die von anderen Unternehmen ausgeführt werden, berücksichtigt?
- Wurden die internen und externen Faktoren, die sich auf das ISMS auswirken können, berücksichtigt?
- Sind Sie sich der Anforderungen beteiligter Parteien, einschließlich regulatorischer und gesetzlicher Vorgaben sowie der Ihrer Kunden, bewusst?
- Wurden die Risiken und Chancen, die mit diesen Faktoren und Anforderungen verbunden sind, berücksichtigt?
- Wurden kontinuierliche Verbesserungsaktivitäten berücksichtigt?

Leitung

- Hat das Topmanagement die Verantwortung für die Wirksamkeit des ISMS angenommen und hat es die Bedeutung eines wirksamen ISMS kommuniziert?
- Wurden Qualitätspolitik und Ziele für das ISMS, die im Einklang mit dem Kontext und der strategischen Ausrichtung des Unternehmens stehen, umgesetzt und kommuniziert?
- Sind die Rollen innerhalb des ISMS klar definiert, vermerkt und kommuniziert?
- Verfügen die Inhaber dieser Rollen über die Befugnis und auch die Zuständigkeit, Konformität und Berichterstattung sicherzustellen?
- Ist ein Programm, das sicherstellt, dass das ISMS seine Ergebnisse, Anforderungen und Ziele erreicht, entwickelt und implementiert worden?

Fortsetzung >>

Planung

Gibt es ein implementiertes System, das den Umgang mit Risiken und Chancen beschreibt, um sicherzustellen, dass das ISMS seine angestrebten Ergebnisse erzielt?

Existiert ein Bewertungsprozess zur Einschätzung des Informationssicherheitsrisikos, der entsprechende Risikoannahmekriterien enthält?

Ist dieser Bewertungsprozess zur Einschätzung des Informationssicherheitsrisikos so beschaffen, dass dieser wiederholbar ist?

Liefert dieser Prozess konsistente, gültige und vergleichbare Ergebnisse?

Hat Ihr Unternehmen Maßnahmen zum Umgang mit diesen Risiken und Chancen eingeplant und diese implementiert?

Ist der Bewertungsprozess zur Einschätzung des Informationssicherheitsrisikos ausreichend, um Risiken aufzudecken, die einen Vertraulichkeits-, Integritäts- und Verfügbarkeitsverlust von Informationen im Anwendungsbereich des ISMS bedeuten würden?

Wurden die Risikoinhaber identifiziert?

Werden die Informationssicherheitsrisiken analysiert, um deren realistische Eintrittswahrscheinlichkeit und die potenziellen Konsequenzen zu ermitteln, und wurden unterschiedliche Risikograde bestimmt?

Werden Informationssicherheitsrisiken mit den festgelegten Risikokriterien abgeglichen und werden diese priorisiert?

Gibt es dokumentierte Informationen über den Bewertungsprozess zur Einschätzung des Informationssicherheitsrisikos und sind diese auch verfügbar?

Hält der Prozess zur Handhabung des Informationssicherheitsrisikos geeignete Optionen bereit?

Wurden Kontrollmaßnahmen zur Umsetzung der gewählten Option zur Handhabung von Risiken definiert?

Wurden die definierten Kontrollmaßnahmen mit dem Anhang A zur ISO/IEC 27001:2013 abgeglichen, um sicherzustellen, dass keine erforderlichen Kontrollmaßnahmen übersehen wurden?

Haben Sie zusammen mit dem Implementierungsstatus der Kontrollmaßnahmen eine Anwendbarkeitserklärung zur Rechtfertigung von Ausschlüssen und Einschlüssen aus dem Anhang A erstellt?

Existiert ein Plan zur Handhabung des Informationssicherheitsrisikos?

- Haben die Risikoinhaber den Plan geprüft und genehmigt?
- Wurden die Restrisiken der Informationssicherheit von den Risikoinhabern genehmigt?
- Wurde dies dokumentiert?

Gibt es einen Plan zur Bestimmung des Änderungsbedarfs an dem ISMS und zu dessen Umsetzung?

Planung – *Fortsetzung*

Wurden messbare Haupt- und Nebenziele des ISMS festgelegt, dokumentiert und in dem gesamten Unternehmen kommuniziert?

Hat Ihr Unternehmen bei der Festlegung der Hauptziele definiert, was wann und von wem erledigt werden muss?

Unterstützung

Hat Ihr Unternehmen die für die Einrichtung, Implementierung, Pflege und kontinuierliche Verbesserung des ISMS (einschließlich Mitarbeiter, Infrastruktur und Umgebung für die Durchführung der Prozesse) erforderlichen Ressourcen festgelegt und bereitgestellt?

Verfügen Sie über einen definierten und dokumentierten Prozess zur Bestimmung der Kompetenzen für die Rollen innerhalb des ISMS?

- Sind dieser Prozess und die Kompetenzen der Mitarbeiter in diesen Rollen dokumentiert?

Hat Ihr Unternehmen das für die einzelnen Rollen innerhalb des ISMS erforderliche Wissen definiert?

Hat Ihr Unternehmen sichergestellt, dass diejenigen Mitarbeiter, die einen Einfluss auf die Leistungsfähigkeit und Wirksamkeit des ISMS haben, über die Kompetenz im Sinne einer geeigneten Ausbildung, Weiterbildung oder Berufserfahrung verfügen, bzw. hat sie Maßnahmen ergriffen, um sicherzustellen, dass diese Mitarbeiter die erforderliche Kompetenz erlangen können?

Wurde die dokumentierte Information, die Teil der Anforderungen der Norm und für eine wirksame Implementierung und den reibungslosen Betrieb des ISMS erforderlich ist, erstellt?

Wird die dokumentierte Information in einer Art und Weise gelenkt, dass sie zugänglich ist, adäquat geschützt, verteilt, abgelegt und aufbewahrt wird, und unterliegt sie dem Änderungsdienst, einschließlich der Dokumente externen Ursprungs, die Ihr Unternehmen im Zusammenhang mit dem ISMS fordert?

Operative Prozesse

Wurden dokumentierte Nachweise geführt, um zu belegen, dass Prozesse wie geplant durchgeführt worden sind?

Gibt es einen Plan zur Bestimmung des Änderungsbedarfs an dem ISMS und zu dessen Umsetzung?

Wenn Änderungen geplant werden, werden diese in einer kontrollierten Art und Weise durchgeführt? Und werden Maßnahmen zur Minimierung unerwünschter Auswirkungen ergriffen?

Werden ausgelagerte Prozesse in geeigneter Weise kontrolliert?

Fortsetzung >>

Operative Prozesse– *Fortsetzung*

Werden Bewertungen des Informationssicherheitsrisikos in geplanten Abständen vorgenommen oder nur dann, wenn es zu wichtigen Änderungen kommt? Und wird dokumentierte Information aufbewahrt?

Hat Ihr Unternehmen Maßnahmen geplant, um mit Risiken und Chancen umzugehen und diese in den Systemprozess zu integrieren?

Wurden diese Maßnahmen dokumentiert?

Bewertung der Leistung

Verfügen Sie über Kriterien zur Evaluierung, Auswahl, Leistungsüberwachung und Reevaluierung Ihrer externen Dienstleister?

Haben Sie bestimmt, was genau überwacht und gemessen werden muss, wann, durch wen, mit welchen Methoden dies geschehen soll, und wann die Ergebnisse ausgewertet werden sollen?

Werden die Ergebnisse der Überwachung und der Messungen dokumentiert?

Werden in regelmäßigen Abständen interne Audits durchgeführt, um zu überprüfen, ob das ISMS wirksam ist und sowohl mit der ISO/IEC 27001:2013 als auch den Anforderungen des Unternehmens konform ist?

Verfügt Ihr Unternehmen über ein Programm zur Durchführung interner Audits des ISMS?

Werden die Ergebnisse dieser Audits an das Management berichtet, dokumentiert und aufbewahrt?

Bewertung der Leistung – *Fortsetzung*

Verfügt Ihr Unternehmen im Falle des Feststellens von Nonkonformitäten über geeignete Prozesse zur Handhabung derselben sowie der damit einhergehenden Korrekturmaßnahmen?

Führt das Topmanagement in regelmäßigen Abständen eine Bewertung des ISMS durch?

Taugt das Ergebnis dieser ISMS-Bewertung durch das Management dazu, Änderungs- und Verbesserungsbedarfe zu identifizieren?

Werden die Ergebnisse der Managementbewertung dokumentiert, befolgt und an betroffene Parteien in geeigneter Weise kommuniziert?

Verbesserung

Wurden Maßnahmen zur Steuerung, Korrektur und Handhabung der Konsequenzen aus den Nonkonformitäten identifiziert?

Wurde zur Beseitigung der Ursache und des Wiederauftretens von Nonkonformitäten der Handlungsbedarf ermittelt?

Wurde ein identifizierter Handlungsbedarf umgesetzt und auf seine Wirksamkeit hin überprüft? Und hat dieser schließlich zur Verbesserung des ISMS geführt?

Wird dokumentierte Information zum Nachweis der Art der Nonkonformitäten, ergriffenen Maßnahmen und Ergebnissen gepflegt?

Erfahren Sie mehr:
Tel.: +49 (0)69 2222 8 9200
Website: bsigroup.de

BSI/DE/MAQ616/IFZS/de

Warum BSI?

By Royal Charter

ISO/IEC 27001:2013 Informations-sicherheits-management

Von Anfang an war BSI bei der Entwicklung der ISO/IEC 27001 in vorderster Reihe mit dabei. Seit der 1995 unter der ursprünglichen Bezeichnung BS 7799 von BSI entwickelten Norm sind wir an der Entstehung dieser Norm und in dem Technischen Komitee der ISO beteiligt. Aus diesem Grund sind wir der beste Ansprechpartner für Sie, wenn es um das Verstehen dieser Norm geht.

BSI erzeugt Exzellenz, indem es Kunden mithilfe von Normen zum Erfolg führt. Wir unterstützen Unternehmen dabei, organisatorisch resilient zu bleiben und verhelfen Ihnen damit zu nachhaltigem Wachstum, der Fähigkeit zur Anpassung an Veränderungen und langfristigem Erfolg.
We make excellence a habit.

Seit über einem Jahrhundert machen unsere Experten Mittelmaß und Nachlässigkeit als größte Herausforderung ausfindig, damit Sie ungehindert Exzellenz erzeugen können in der Art und Weise, wie Menschen arbeiten und Produkte funktionieren. Mit 80.000 Kunden in 182 Ländern ist BSI eine Organisation, deren Normen Exzellenz in der ganzen Welt fördern.

Unsere Produkte und Dienstleistungen

Wir verfügen über ein einzigartiges Portfolio an sich ergänzenden Produkten und Dienstleistungen, die allesamt unter unseren drei Geschäftsfeldern geführt werden: Wissen, Sicherheit und Konformität.

Wissen

Der Kern unseres Geschäfts konzentriert sich auf das Wissen, das wir bei unseren Kunden schaffen und vermitteln. Im Bereich der Normen bauen wir unsere Reputation als Fachinstitution, die Experten aus allen Branchen zusammenführt, um Normen auf lokaler, regionaler und internationaler Ebene zu entwickeln, kontinuierlich aus. So stammen acht der zehn weltweit wichtigsten Managementsystemnormen von BSI.

Sicherheit

Unabhängige Überprüfungen der Konformität eines Prozesses oder eines Produktes nach einer spezifischen Norm gewährleisten, dass unsere Kunden auf einem Niveau höchster Exzellenz operieren. Wir schulen unsere Kunden in den weltweit führenden Implementierungs- und Audit-Methoden, um sicherzustellen, dass sie aus unseren Normen den maximalen Nutzen erzielen.

Konformität

Zur Erzielung realer, langfristiger Vorteile müssen unsere Kunden permanente Konformität mit den gesetzlichen Vorgaben, den Marktanforderungen oder mit den Normen sicherstellen, sodass Konformität zur Gewohnheit wird. Zudem bieten wir spezialisierte Managementtools zur Unterstützung dieses Prozesses.

bsi.

Erfahren Sie mehr:
Tel.: +49 (0)69 2222 8 9200
Website: bsigroup.de