VORBEREITUNG AUF DAS ISO-ZERTIFIZIERUNGSAUDIT: EIN LEICHT VERSTÄNDLICHER DEUTSCHER LEITFADEN

ISO TASCHEN BUCH SERIE

03

Eine Schritt-für-Schritt-Anleitung für ISO-Praktiker in Kleinunternehmen

DEJAN KOSUTIC

Vorbereitung auf das ISO-Zertifizierungsaudit: Ein leicht verständlicher deutscher Leitfaden

Ebenfalls von Dejan Kosutic:

Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own

9 Steps to Cybersecurity: The Manager's Information Security Strategy Manual

Becoming Resilient: The Definitive Guide to ISO 22301 Implementation

Dejan Kosutic

Vorbereitung auf das ISO-Zertifizierungsaudit: Ein leicht verständlicher deutscher Leitfaden

Eine Schritt-für-Schritt-Anleitung für ISO-Praktiker in Kleinunternehmen

Advisera Expert Solutions Ltd
Zagreb, Kroatien

Erstmals veröffentlicht von Advisera Expert Solutions Ltd
Zavizanska 12, 10000 Zagreb
Kroatien
Europäische Union
http://advisera.com/

ISBN: 978-953-8155-09-3

Erstauflage, 2017

Originaltitel: Preparing for ISO Certification Audit: A Plain English Guide

Übersetzt aus dem Englischen von Eva Weber

ÜBER DEN AUTOR

Dejan Kosutic ist Autor zahlreicher Artikel, Video-Tutorials, Dokumentationsvorlagen, Webinars und Kurse über ISO 27001, ISO 22301 und anderer ISO-Standards. Er ist Autor des führenden ISO 27001- & ISO 22301-Blog und hat unterschiedlichsten Organisationen, einschließlich Finanzinstituten, Regierungsbehörden und IT-Unternehmen, geholfen, Informationssicherheitsmanagement entsprechend diesen Standards zu implementieren. Er besitzt zahlreiche Zertifikate, unter anderem die Zertifikate „ISO 27001 Lead Auditor“ und „ISO 9001 Lead Auditor“.

Klicken Sie hier, um sein LinkedIn-Profil zu sehen.

INHALTSVERZEICHNIS

VORWORT

Als mein Buch *Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own* Anfang des Jahres publiziert wurde, realisierte ich bald, dass es viele Leute lasen, weil sie in erster Linie daran interessiert waren, wie sie Ihr Unternehmen auf die ISO-Zertifizierung vorbereiten können.

Aus diesem Grund habe ich dieses kurze Buch, als Teil der Handbuch-Serie, geschrieben, das nur auf die Themen Zertifizierungsprozess und wie man sich darauf vorbereitet ausgerichtet ist. Dieses Buch ist nicht nur auf ISO 27001 fokussiert – der Zertifizierungsprozess ist der gleiche für jeden Standard, daher habe ich dieses Buch derart erstellt, dass es für ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 22000, OHSAS 18001, ISO 13485 und IATF 16949 perfekt zulässig ist.

Dieses Buch, *Vorbereitung auf den ISO-Zertifizierungsaudit: Ein leicht verständlicher deutscher Leitfaden,* ist eigentlich ein Auszug aus dem Buch *Secure & Simple,* das die Zertifizierung behandelt. Sie finden hier die gleichen Abschnitte, mit beinahe dem gleichen Text – der Text wurde, wie gesagt, derart angepasst, dass er nach den Gesichtspunkten jedes ISO-Standards lesbar ist.

Warum also zwei Bücher mit fast dem gleichen Text? Weil ich ein schnell zu lesendes Buch bieten wollte für Leute, die nur auf die Vorbereitung für die Zertifizierung fokussiert sind und nicht die Zeit (oder Notwendigkeit) haben, ein ausführliches Buch über die ISO-Implementierung, d.h. ein Buch wie *Secure & Simple*, zu lesen.

Vielleicht sind Sie auch verwundert darüber, dass dieses Buch ziemlich kurz ist, wo es doch andere Bücher am Markt gibt, die

viel ausführlicher und detaillierter sind. Ist es wirklich möglich, ein solch komplexes Thema in einem kurzen Buch wie diesem zu erklären? Nun ja, dazu gibt es zwei Antworten:

Erstens ist dieses Buch auf die Vorbereitung für das Zertifizierungsaudit in kleineren Unternehmen ausgerichtet – daher habe ich mit Absicht die Schritte vereinfacht, so dass Ihre Vorbereitungen ziemlich rasch erledigt werden können, und alle Elemente, die nur für größere Unternehmen benötigt werden würden, ausgelassen.

Zweitens, und das ist noch wichtiger, folgte ich meinem Unternehmensleitbild: „Wir machen komplexe Gefüge leicht verständlich und einfach anwendbar." Mit anderen Worten, es ist leicht, Dinge zu verkomplizieren, doch ist es schwierig, Dinge leicht verständlich zu machen. Wenn Sie daher mit dem Lesen dieses Buches beginnen, werden Sie bemerken, dass ich all das schwer zu verstehende Gerede und alle unnötigen Details eliminiert habe und den Fokus darauf richtete, was genau getan werden muss. Und das in einer für Anfänger, mit keinerlei vorherigen Erfahrung in der Implementierung von ISO-Standards, verständlichen Sprache.

Seien Sie daher versichert: wenn Sie eine kleinere Organisation sind, werden Sie durch Verwendung dieses Buches in der Lage sein, sich für das Zertifizierungsaudit zu rüsten. Und Sie werden den echten Nutzen der Zertifizierung für Ihr Unternehmen erfahren.

1
EINFÜHRUNG

Weshalb würde sich Ihr Unternehmen zu einer ISO-Zertifizierung entschließen? Wie unterscheidet sich die Unternehmenszertifizierung von der Personenzertifizierung? Und, ist dieses Buch die richtige Wahl für Sie?

Dieses Buch deckt den Zertifizierungsprozess für alle ISO-Managementstandards ab - ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 13485, jedoch auch OHSAS 18001 und IATF 16949 (früher ISO/TS 16949), daher beziehe ich mich in diesem Bauch auf "ISO-Standard", oder einfach nur "Standard", um alle diese Standards abzudecken.

1.1 Warum sollte sich Ihr Unternehmen zu einer ISO-Zertifizierung entschließen?

Bevor Sie sich entscheiden, ob sich Ihr Unternehmen zu einer Zertifizierung entschließt, müssen Sie sich eine wichtige Frage stellen: brauchen Sie das wirklich?

Ich muss Ihnen sagen, dass es viele Organisationen gibt, welche den Standard ohne Zertifizierung implementierten – ein augenscheinliches Beispiel sind Banken und andere Finanzinstitutionen. In den meisten Ländern sind die Bestimmungen derart, dass sie sehr strenge Informationssicherheitsverfahren und Absicherungsmaßnahmen implementieren müssen und die Mehrheit von ihnen hat das durch den Einsatz von ISO 27001 getan. Doch wenige davon wurden zertifiziert – sie kamen zum Schluss, dass es für sie keine geschäftlichen Gründe gibt, dies zu tun.

Und das ist genau das, was Sie tun müssen – überlegen Sie genau, ob Sie das Zertifikat brauchen. Hier die potentiellen Gründe, warum Sie die Zertifizierung sinnvoll finden könnten:

1) Marketing. Sie können das Zertifikat nutzen, um neue Kunden zu bekommen (z.B. wegen Ausschreibungen), oder um im Geschäft zu bleiben (z.B. haben bereits alle Ihre Mitbewerber das Zertifikat).

2) Compliance. In seltenen Fällen werden die Bestimmungen von Ihnen verlangen, einen bestimmten ISO-Standard zu implementieren, Sie könnten jedoch Fälle haben, in denen Sie einen Vertrag mit Kunden abschließen, der sie verpflichtet, z.B. ein mit ISO 9001 konformes Qualitätsmanagementsystem zu implementieren. Und anstatt die Auditoren von jedem Ihrer Kunden, die überprüfen wollen, ob Sie den Vertrag erfüllt haben, zu ertragen, können Sie den Zertifizierungsauditor diesen Job erledigen lassen und dann allen das Zertifikat vorzeigen.

3) Interner Druck. In manchen Unternehmen endet diese Art von Projekten niemals ohne starken Druck – z.B. einem klaren Termin. Wenn Sie sich daher mit der Zertifizierungsstelle auf ein fixes Datum für das Zertifizierungsaudit einigen, werden sowohl Ihr Management als auch Ihre Mitarbeiter einen viel stärkeren Handlungsdruck zur Fertigstellung des Projekts haben.

4) Objektive Beiträge. Wenn Sie Ihre Informationssicherheit auf die bestmögliche Art und Weise implementiert haben möchten, ist es gut, Leute mit großer Erfahrung beizuziehen, die wissen, wie Sie mit den Besten der Branche mithalten können. Die Zertifizierungsauditoren können Inputs liefern, worin Sie sich verbessern könnten.

Wenn Sie daher zumindest einen dieser Vorteile als für Ihr Unternehmen zutreffend fanden, sollten Sie sich wahrscheinlich für die Zertifizierung entscheiden, aber das Gegenteil trifft ebenfalls zu: wenn Sie sich in keinem dieser Punkte wiederfinden, braucht Ihr Unternehmen das Zertifikat wahrscheinlich gar nicht.

1.2 Zertifizierung gegenüber Registrierung gegenüber Akkreditierung

Ehe wir tiefer in das Thema der Zertifizierung eintauchen, lassen Sie uns zuerst einige grundlegende Dinge klären.

Wie die Unternehmenszertifizierung funktioniert. Zunächst, ISO-Standards werden von der International Organization for Standardization publiziert – das ist eine internationale, von Regierungen rund um die Welt gegründete Einrichtung. Ihr Zweck ist, Standards, als Möglichkeit der Weitergabe von Wissen und bewährten Methoden, zu publizieren – zum jetzigen Zeitpunkt sind insgesamt fast 20.000 Standards publiziert und in jedem Land anerkannt.

Die ISO-Managementstandards sind nur Teil dieser 20.000 Standards, die in erster Linie als Hilfe für Unternehmen zur Verbesserung von deren Betrieb in bestimmten Bereichen (z.B. ISO 9001 für Qualitätsmanagement, ISO 27001 für Informationssicherheitsmanagement, etc.) erstellt wurden – das ist der Grund, warum sich die meisten Vorträge über diese Standards auf Unternehmen und deren Registrierung, Zertifizierung und Akkreditierung beziehen.

Zertifizierung gegenüber Registrierung. Wenn man sagen möchte, dass ein Unternehmen einen Standard implementiert hat (z.B. ein Umweltmanagementsystem entsprechend ISO 14001), das Zertifizierungsaudit erfolgreich absolviert hat und

die Zertifizierungsstelle das Zertifikat ausgestellt hat, würde man das normalerweise als Registrierung oder Zertifizierung bezeichnen.

In Nordamerika wird der Begriff "Registrierung" am häufigsten verwendet, während es im Rest der Welt üblicherweise „Zertifizierung" genannt wird. Gibt es also einen Unterschied? Technisch ja, doch im Wesentlichen nein.

Eine Zertifizierung ist, wenn eine Zertifizierungsstelle ein Zertifikat ausstellt, das nachweist, dass ein Unternehmen mit dem Standard konform ist; eine Registrierung ist, wenn das Zertifikat bei der Zertifizierungsstelle registriert ist. Es kommt daher auf das Gleiche raus – ein Unternehmen erhielt ein Zertifikat, das formal anerkannt ist.

Übrigens empfiehlt die International Organization for Standardization die Verwendung der Bezeichnung "Zertifizierung", daher werde ich von nun an in diesem Buch diesen Ausdruck verwenden.

Zertifizierungsstelle gegenüber Registrator. Das ist der Terminologie-Unterschied, der sich direkt von der Verwendung der Ausdrücke „Zertifizierung/Registrierung" ableitet – in Nordamerika verwenden die Leute üblicherweise den Ausdruck „Registrator", während das im Rest der Welt „Zertifizierungsstelle" genannt wird.

Aber nochmals, dabei handelt es sich um ein und die gleiche Sache – es sind die Institutionen, welche die Zertifizierungsaudits durchführen und die Zertifikate ausstellen. Auch hier empfiehlt die ISO die Verwendung des Ausdrucks „Zertifizierungsstelle".

Akkreditierung gegenüber Zertifizierung. Und was ist dann die Akkreditierung? Um Zertifizierungsaudits durchführen zu können und Zertifikate auszustellen, muss die Zertifizierungsstelle eine Lizenz erhalten – und diese Lizenz wird

„Akkreditierung" genannt. Zertifizierungsstellen werden daher akkreditiert, während Unternehmen zertifiziert werden. (Die Zertifizierungsstelle muss mit dem Standard ISO 17021 konform sein, wenn sie für die Zertifizierung von Managementsystemen akkreditiert werden will.)

Es gibt normalerweise nur eine Akkreditierungsstelle für jedes Land (z.B. UKAS für das Vereinigte Königreich), während es in jedem Land mehrere operierende Zertifizierungsstellen gibt – von kleinen lokalen Zertifizierungsstellen bis zu großen, multinationalen Gesellschaften, wie SGS, BSI, DNV, Bureau Veritas, etc.

Die gute Sache an Akkreditierungsstellen ist, dass sie üblicherweise die Liste akkreditierter Zertifizierungsstellen in ihrem Land publizieren – sehen Sie hier die Liste von Zertifizierungsstellen im Vereinigten Königreich , und hier die Liste von Zertifizierungsstellen in den Vereinigten Staaten.

Übrigens müssen die Akkreditierungsstellen ebenfalls mit dem Standard konform sein – das ist ISO 17011, ein Standard, der den Prozess der Akkreditierung definiert.

Zertifizierung für Personen. Alles oben Gesagte galt für die Zertifizierung von Unternehmen – wenn Sie sich zu einer Personenzertifizierung entschließen, liegen die Dinge etwas anders. Viele Schulungen für ISO-Standards wurden entwickelt, um zu helfen, einen Standard in einem Unternehmen zu implementieren und dieses zu auditieren. Das ist auch der Grund, warum es zu dieser Schulungsbranche zugehörige Zertifizierungen und Akkreditierungen gibt.

Die Akkreditierung betreffend gibt es ein ähnliches Schema wie oben beschrieben – will eine Institution Schulungszertifikate ausstellen, sollte sie durch eine Akkreditierungsstelle akkreditiert

sein, und in diesem Fall muss eine derartige Institution mit ISO 17024 konform sein.

Hier einige der gängigsten akkreditierten Schulungsinstitutionen: PECB, IRCA, Exemplar Global (früher RABQSA), etc.

Personenzertifizierung gegenüber Schulungszertifizierung. In den meisten Fällen führen diese akkreditierten Institutionen die Kurse für Studenten nicht direkt durch, sondern haben ein Partner-Netzwerk – Schulungsanbieter -, welche die Kurse unter ihrer Lizenz und Aufsicht durchführen.

Diese Beziehung zwischen akkreditierten Institutionen und Schulungsanbietern funktioniert normalerweise auf zwei Arten:

(a) die Schulungsanbieter verwenden Kurse, die von den akkreditierten Institutionen entwickelt wurden und danach stellen die akkreditierten Institutionen direkt an die Studenten Zertifikate aus, oder (b) die Schulungsorganisation entwickelt ihre eigenen Kurse und eine akkreditierte Institution zertifiziert diese Kurse – in diesem Fall ist es bei Schulungsorganisationen üblich, das Zertifikat an die Studenten auszustellen, mit Genehmigung der akkreditierten Institution.

Es gibt weltweit unzählige Schulungsorganisationen – von den Zertifizierungsstellen, welche auch die Zertifizierung von Organisationen anbieten, bis hin zu kleinen, spezialisierten Nischenplayern und Anbietern von Online-Kursen.

Erwähnenswert ist, dass die Zertifizierung von Kursen für Schulungsanbieter, die Kurse wie "Lead Auditor" anbieten, verpflichtend ist, da dies die einzige Möglichkeit ist, von Zertifizierungsstellen anerkannt zu werden, die Auditoren mit solchen Zertifikaten einstellen. Allerdings entscheiden sich Schulungsanbieter bei anderen, kürzeren Kursen oft, ihre Kurse nicht zu zertifizieren, weil eine solche Anerkennung nicht so

wichtig ist und sie ihren Markennamen als ausreichend für eine Garantie der Kursqualität erachten.

1.3 Wer sollte dieses Buch lesen?

Dieses Buch wurde in erster Linie für Anfänger auf diesem Gebiet und für Leute mit moderatem Wissen über die ISO-Zertifizierung geschrieben – ich habe dieses Buch so strukturiert, dass jemand mit keinerlei vorheriger Erfahrung oder keinem Wissen über ISO-Standards schnell verstehen kann, wie der gesamte Zertifizierungsprozess funktioniert und was die Schritte für einen erfolgreichen Abschluss sind. Wenn Sie aber Erfahrung mit der ISO-Zertifizierung haben, jedoch das Gefühl haben, noch immer Wissenslücken aufzuweisen, werden Sie dieses Buch ebenfalls hilfreich finden.

Sind Sie also ein mit der Implementierung eines ISO-Standards in einem kleinen oder mittleren Unternehmen betrauter Produktionsleiter, Ingenieur, Compliance-Beauftragter, Informationssicherheitsexperte, Leiter der IT-Abteilung, Vorstand oder ein Projektmanager, ist dieses Buch perfekt für Sie.

Ich glaube, dieses Buch wird auch durchaus nützlich für Berater sein – da ich selbst Berater bin, habe ich mich bemüht, den logischsten Weg zur Vorbereitung auf das Zertifizierungsaudit darzustellen. Sie werden sich so durch gründliche Lektüre dieses Buches das Know-how für Ihre zukünftigen Beratungsaufträge erwerben.

1.4 Was dieses Buch nicht ist

Dieses Buch behandelt die Zertifizierung von Unternehmen und nicht, wie Personen zu zertifizieren sind – auch wenn sowohl Unternehmen, als auch Personen ein ISO-Zertifikat bekommen

können, sind der Zweck und der Prozess für die Zertifizierung sehr unterschiedlich.

Der Fokus dieses Buches ist auf die Schritte im Zertifizierungsprozess gerichtet und wie man sich auf die Zertifizierung vorbereitet, es erklärt aber nicht, wie der Standard zu implementieren ist – im Abschnitt 2.1 finden Sie Verknüpfungen zu Artikeln, welche die Schritte in der Implementierung erklären.

Dieses Buch liefert Ihnen keine fertigen Vorlagen für alle Ihre Richtlinien, Verfahren und Pläne, allerdings erklärt dieses Buch, nach welchen Dokumenten der Zertifizierungsauditor suchen wird.

Dieses Buch ist keine Kopie eines ISO-Standards – Sie können durch Lesen dieses Buchs nicht das Lesen des Standards ersetzen. Dieses Buch ist dafür gedacht, zu erklären, wie der Standard zu interpretieren ist (weil der Standard eher unfreundlich geschrieben ist) und welche Art von Compliance der Auditor zu sehen erwartet.

Machen Sie daher bitte nicht den Fehler, eine Implementierung und Zertifizierung gegen einen Standard zu beginnen, ohne diesen tatsächlich gelesen zu haben – ich glaube, Sie werden dieses Buch und den ISO-Standard als perfekte Kombination für Ihre zukünftige Arbeit empfinden. Den Standard können Sie auf der offiziellen Website von ISO kaufen.

1.5 Zusätzliche Ressourcen

Hier sind einige Ressourcen, die Ihnen – zusammen mit diesem Buch – helfen werden, mehr über die verschiedenen ISO-Standards zu lernen:

- ISO Online-Kurse – kostenlose Online-Schulungen, in denen Sie die Grundlagen von ISO 9001, ISO 14001 und ISO 27001 lernen, einschließlich Tipps dazu, wie man sich für die Zertifizierung entscheidet.

- ISO 27001 kostenlose Downloads ISO 9001 kostenlose Downloads und ISO 14001 kostenlose Downloads – eine Sammlung von Weißpapieren, Checklisten, Diagrammen, Vorlagen, etc.

- Conformio – Cloud-basiertes Dokumenten-Managementsystem (DMS) und Projektmanagement-Tool, fokussiert auf ISO-Standards.

- ISO 27001 Dokumentations-Toolkit – ein Set aller Dokumentationsvorlagen, die für ISO 27001 erforderlich sind, mit inkludierter Experten-Unterstützung, die Sie Schritt für Schritt in Richtung Zertifizierung bringt; ähnliche Toolkits gibt es auch für andere ISO-Standards.

- Offizielle ISO-Website – hier können Sie eine offizielle Version von jedem ISO-Standard kaufen.

2
SICHERSTELLUNG, DASS IHR UNTERNEHMEN DAS ZERTIFIZIERUNGSAUDIT BESTEHT

Offen gesagt habe ich noch niemanden getroffen, der an der Zertifizierung Freude hat. In den meisten Fällen wird sie von allen als notwendiges Übel betrachtet und der Tag, an dem der Auditor schließlich eintrifft, wird gehasst. (Oder man meldet sich krank an diesem Tag.)

Es muss aber nicht so sein – es kann Ihnen, neben der Zertifizierung selbst, etwas bringen – was ich später erklären werde. Zertifizierungsauditoren sind erfahrene Leute mit einem perfekten Überblick über die besten Praktiken und Sie können von ihnen eine Menge lernen, doch müssen Sie auf die richtige Art auf sie zugehen.

2.1 Schritte, ehe man sich für die Zertifizierung entscheidet – die letzte Kontrolle

Selbstverständlich müssen Sie vor der Entscheidung für die Zertifizierung den Standard implementieren. Da dieses Buch nicht für eine Beschreibung der Implementierung vorgesehen war, finden Sie hier einige Links zu Artikeln, die Ihnen bei der Implementierung helfen werden:

- Checkliste der ISO 9001 Implementierungs- & Zertifizierungsschritte
- Liste der ISO 14001 Implementierungsschritte
- ISO 27001 Implementierungs-Checkliste
- 17 Schritte zur Implementierung von ISO 22301
- 12 Schritte für die ISO 20000-Imlementierung
- 12 Schritte für die Implementierung und Zertifizierung gegen OHSAS 18001

OK, Sie haben nun seit Monaten an der ISO-Implementierung gearbeitet, versucht herauszufinden, wie Sie es sich leichter machen können, indem Sie Bücher und Artikel lasen, haben nicht nur Ihre Kollegen, sondern auch Ihr Management überzeugt, dass dieser Standard äußerst nützlich ist und haben dennoch noch immer ein Problem: Sie sind voreingenommen.

Dieses Projekt ist Ihr Baby und Sie neigen vielleicht dazu zu glauben, dass die Dokumente und alles, was Sie vorbereiteten, einwandfrei sind. Jedoch stimmt das niemals – Sie haben immer etwas vernachlässigt, Sie könnten sogar manche Anforderungen falsch verstanden haben oder Sie könnten etwas übersehen haben. Möglicherweise liegt das Problem nicht bei Ihnen – vielleicht gibt es jemanden, der z.B. für die Messung verantwortlich ist, doch erledigt diese Person den Job nicht ordentlich.

All das bedeutet, dass Sie bei der Zertifizierung Probleme haben könnten. Um dies zu vermeiden, würde ich Ihnen empfehlen, eine letzte Kontrolle vorzunehmen, die Ihnen ein klares Bild geben sollte, was Sie vor der Zertifizierung noch in Ordnung bringen sollten.

Im Wesentlichen ist dies der Trick:

- Überprüfen Sie zuerst, ob das interne Audit, Management Review und Korrekturmaßnahmen durchgeführt wurden.
- Dann gehen Sie die Liste obligatorischer Dokumente durch und schauen, ob Sie alles haben. Diese Artikel werden Ihnen dabei helfen:
    - Liste erforderlicher obligatorischer Dokumente für ISO 9001:2015
    - Liste erforderlicher obligatorischer Dokumente für ISO 14001:2015
    - Liste erforderlicher obligatorischer Dokumente für ISO 27001 (2013-Überarbeitung)
    - Erforderliche obligatorische Dokumente für ISO 22301
    - Liste erforderlicher obligatorischer Dokumente für OHSAS 18001
- Überprüfen Sie, ob alle **Prozesse und Kontrollen, die Sie geplant haben, implementiert wurden** – z.B. werden in ISO 27001 die Kontrollen durch das Dokument mit dem Namen „Risikobehandlungsplan“ geplant.
- Als Nächstes lesen Sie den Standard noch einmal und schauen Sie, ob Ihre **Dokumentation mit allen Anforderungen** im Standard übereinstimmt.
- Und schließlich kommt der schwierigste Teil – Sie müssen **durch Ihr Unternehmen gehen** (Sie sollen auch einige Ihrer Partner/Lieferanten, die in Ihrem System eine Rolle spielen, aufsuchen) und sich so verhalten, als wären Sie

der Zertifizierungsauditor. Das bedeutet im Grunde genommen, dass Sie ihnen immer wieder die eine simple Frage stellen müssen: Führen Sie alles durch, was in der Dokumentation geschrieben steht? Sie müssen nur lesen, was jedes einzelne Ihrer Dokumente sagt (Richtlinien, Verfahren, Pläne, etc.) und überprüfen, ob die Antworten, die Sie erhalten, passend sind. Um die Wahrheit herauszufinden, sollten Sie sich nicht nur auf deren Antworten verlassen – Sie müssen noch tiefer schürfen und nach Aufzeichnungen suchen, die belegen, was sie sagen.

Und das ist es – sobald Sie diese Aufgaben für jede Ihrer Aktivitäten, für jedes Ihrer Dokumente und für jeden Ihrer hauptsächlichen Lieferanten und Partner erledigen, werden Sie ein ziemlich gutes Bild darüber haben, was funktioniert und was korrigiert werden muss.

Bei näherer Betrachtung werden Sie herausfinden, dass diese Schritte den Schritten, welche vom internen Auditor durchgeführt werden, sehr nahekommen. Sie fragen, warum man das also tun sollte? Erstens deshalb, weil alle internen Auditoren für gewöhnlich unerfahrene Leute sind und Sie von ihnen bei deren erstem Job nicht zu viel erwarten dürfen. Und zweitens, weil es Sie sind, der für den Erfolg des Projekts verantwortlich ist und Sie wahrscheinlich sicherstellen möchten, dass alles fertig ist.

Sie können auch jemand Externen für die Durchführung der letzten Kontrolle anheuern – das kann durch Ihren Berater erledigt werden, falls Sie einen haben – es stimmt zwar, dass er das interne Audit aus Interessenskonflikten nicht durchführen kann, doch hält Sie niemand davon ab, ihn für diese letzte Kontrolle anzuheuern. Und wenn der Berater Erfahrung mit Auditierungen hat, noch besser.

Sehen Sie sich bitte auch die Mini-Fallstudie in Kapitel 3 an: Mini-Fallstudie: Vorbereitung eines Telekom-Unternehmens auf die Zertifizierung.

2.2 Wie man eine Zertifizierungsstelle auswählt

Natürlich ist der Preis das Hauptkriterium bei der Auswahl der Zertifizierungsstelle und natürlich sollten Sie eine Reihe von Zertifizierungsstellen um ein Angebot bitten, um zu sehen, was in deren Preis inkludiert ist.

Allerdings ist der Preis nicht alles – hier sind einige andere, zu berücksichtigende Dinge, wenn Sie sich entscheiden, mit wem Sie zusammenarbeiten möchten:

- Reputation. Wenn Sie Ihr Zertifikat für Marketingzwecke nutzen wollen, möchten Sie Ihr Zertifikat vermutlich nicht von einer Stelle bekommen, die bekannt dafür ist, dieses ohne irgendwelche Kriterien auszustellen. Sie sollten eine Zertifizierungsstelle mit solider, wenn nicht perfekter, Reputation wählen.

- Akkreditierung. Genau genommen, kann Ihnen jeder ein Stück Papier geben, welches besagt, dass Sie ISO-zertifiziert sind, doch leider ist nicht jede Zertifizierungsstelle akkreditiert, das zu tun – daher müssen Sie überprüfen, ob die Zertifizierungsstelle eine Akkreditierung hat.

- Spezialisierung. Wenn Sie eine Bank sind, ist es ehrlich gesagt keine gute Idee, eine Zertifizierungsstelle zu haben, die bisher nur Produktionsunternehmen zertifizierte. Hat der Auditor bisher nur Produktionsunternehmen zertifiziert, verlieren Sie für Erklärungen, wie die Bank arbeitet, zu viel Zeit – Ergebnis

(Dieser Abschnitt des Buches ist in der kostenlosen Vorschau nicht verfügbar)

LITERATURVERZEICHNIS

ISO 9001:2015, Quality management systems – Requirements

ISO 14001:2015, Environmental management systems – Requirements with guidance for use

ISO/IEC 20000-1:2011, Information technology – Service management – Part 1: Service management system requirements

ISO 22301: 2012, Societal security – Business continuity management systems – Requirements

ISO/IEC 27001:2013, Information technology – Security techniques – Information security management systems – Requirements

ISO/IEC 27002:2013, Information technology – Security techniques – Code of practice for information security controls

ISO 31000:2009, Risk management – Principles and guidelines

http://advisera.com/27001academy/blog/ *ISO 27001 & ISO 22301 Blog*, Advisera.com

http://training.advisera.com/course/iso-27001-internal-auditor-course/ *ISO 27001 Internal Auditor Course*, Advisera.com

INDEX

Vorbereitung auf das ISO-Zertifizierungsaudit: Ein leicht verständlicher deutscher Leitfaden

Eine Schritt-für-Schritt-Anleitung für ISO-Praktiker in Kleinunternehmen

Denken und agieren Sie mit diesem umfassenden, praktischen Schritt-für-Schritt-Leitfaden für die Zertifizierung gegen ISO 9001, ISO 14001, ISO 27001 oder jeden anderen ISO Management-Standard wie ein erfahrener Praktiker.

Der Autor und erfahrene Berater Dejan Kosutic teilt sein Wissen und seine praktische Erfahrung mit Ihnen in einem unbezahlbaren Buch. Sie lernen das Folgende:

- ✓ Die Vorteile der ISO-Zertifizierung für Ihr Unternehmen
- ✓ Alle Schritte im ISO-Zertifizierungsprozess
- ✓ Wie man die Zertifizierungsstelle auswählt
- ✓ Was der Zertifizierungsauditor tun und was er nicht tun kann
- ✓ Wie Nichtkonformitäten zu behandeln sind
- ✓ Wie man auf den Zertifizierungsauditor zugeht
- ✓ All das, und noch viel mehr…

Geschrieben in leicht verständlicher Sprache, ist *Vorbereitung auf das ISO-Zertifizierungsaudit: Ein leicht verständlicher deutscher Leitfaden* für Leute gedacht, die das erste Mal eine ISO-Zertifizierung in Angriff nehmen und klare Anleitungen benötigen, wie dies zu tun ist. Ob Sie nun ein erfahrener Praktiker sind oder neu auf dem Gebiet, dies ist das einzige Buch, das Sie jemals zu diesem Thema brauchen werden.