MANAGEMENT DER ISO-DOKUMENTATION: EIN LEICHT VERSTÄNDLICHER DEUTSCHER LEITFADEN

ISO

TASCHEN BUCH SERIE

04

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

DEJAN KOSUTIC

Management der ISO-Dokumentation: 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

ISO 27001 Risk Management in Plain English

ISO 27001 Annex A Controls in Plain English

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

ISO Internes Audit: Ein leicht verständlicher deutscher Leitfaden

Dejan Kosutic

Management der ISO-Dokumentation: 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: 978-953-8155-10-9

Erstauflage, 2017

Originaltitel: Managing ISO Documentation: 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* vergangenes Jahr publiziert wurde, realisierte ich bald, dass es viele Leute lasen, weil sie daran interessiert waren, zu erfahren, wie sie die Dokumentation managen könnten.

Aus diesem Grund habe ich dieses kurze Buch, als Teil der Handbuch-Serie, geschrieben, das nur darauf ausgerichtet ist, wie man Richtlinien, Verfahren, Pläne und andere Dokumente und Aufzeichnungen handhabt. Dieses Buch ist nicht nur auf ISO 27001 fokussiert – die Regeln für die Handhabung von Dokumenten sind die gleichen 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, *Management der ISO-Dokumentation: Ein leicht verständlicher deutscher Leitfaden,* ist eigentlich ein Auszug aus dem Buch *Secure & Simple* und wurde nur mit einigen kleineren Details aufbereitet. Wenn Sie es daher mit den Abschnitten von *Secure & Simple* vergleichen, welche die Dokumentation behandeln, werden Sie hier die gleichen Abschnitte finden, mit fast dem gleichen Text - wie bereits erwähnt, der Text wurde so aufbereitet, dass er nach den Gesichtspunkten jedes ISO-Standards lesbar ist.

Warum also zwei Bücher mit beinahe dem gleichen Text? Weil ich eine schnelle, schriftliche Referenz für Leute bieten wollte, die ihren Fokus nur auf das Management der Dokumentation richten und nicht die Zeit (oder Erfordernis) haben, ein ausführliches Buch über die ISO-Implementierung, d.h. ein Buch wie *Secure & Simple*, zu lesen.

Vielleicht sind Sie auch darüber erstaunt, dass dieses Buch so kurz ist, wo es doch am Markt andere Bücher über die ISO-Dokumentation gibt, die ausführlicher und detaillierter sind. Ist es wirklich möglich, ein derart komplexes Thema in einem kurzen Buch wie diesem zu erklären? Nun ja, darauf gibt es zwei Antworten:

Erstens ist dieses Buch auf das Management der Dokumentation in kleineren Unternehmen fokussiert – deshalb habe ich die Beschreibung mit Absicht vereinfacht, so dass Sie das Dokument auf einfache Weise handhaben 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, Dokumente auf die optimalste Art und Weise zu managen. Und Sie werden den echten Nutzen erkennen, die passenden Dokumente zu haben, die Ihnen bei der Ausübung Ihrer Geschäftstätigkeit helfen werden.

1
EINFÜHRUNG

Warum brauchen Sie Dokumente und Aufzeichnungen (oder „dokumentierte Informationen, wie diese beiden in ISO-Standards genannt werden)? Ist dieses Buch die richtige Wahl für Sie?

Dieses Buch umfasst Tipps zur Handhabung der Dokumentation für alle ISO-Managementstandards - ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 13485, aber auch OHSAS 18001 und IATF 16949 (früher ISO/TS 16949), daher beziehe ich mich im Buch auf „ISO-Standard", oder einfach „Standard", um jeden dieser Standards abzudecken.

1.1 Warum ist die Dokumentation für ISO-Managementsysteme wichtig?

Das vielleicht umstrittenste Thema bei ISO-Standards ist die Dokumentation – es gibt dazu viele verschiedene, sehr oft vollkommen gegensätzliche, Meinungen:

- "Wir brauchen diese Dokumente nicht – wir sind ohne diese ganz gut unterwegs, das wäre nur zu viel des Guten."
- "In diesen Standards geht es nur um Dokumentation – wir brauchen nur die Dokumente auszufüllen und erhalten automatisch das Zertifikat."
- "Wir müssen Richtlinien und Verfahren für jeden einzelnen Prozess, jede Aktivität und alle Kontrollen in unserem Unternehmen erstellen – je mehr Dokumente,

desto klarer werden die Regeln sein und es wird für uns einfacher, allem zu entsprechen."

Leider sind Aussagen wie diese sehr oft zu hören. Und leider gibt keine davon in Wahrheit wieder, was ISO-Standards tatsächlich verlangen.

Der Schwerpunkt der Implementierung eines Standards ist, dass die Mitarbeiter ihre Aktivitäten auf bessere Art und Weise durchführen und die Dokumentation ist dazu da, zu helfen, dies zu tun, da ihre Prozesse und Aktivitäten ansonsten unkontrollierbar werden würden. Auch die Aufzeichnungen, die produziert werden, werden Ihnen helfen zu messen, ob Sie Ihre Ziele erreichen und Ihnen ermöglichen, jene Aktivitäten, welche die Erwartungen nicht erfüllen, zu korrigieren.

Sie sollten deshalb die Dokumentation nur als Tool zum Erreichen von besserer Qualität (mit ISO 9001), Sicherheit (mit ISO 27001), Umweltschutz (ISO 14001) etc. betrachten – es geht nicht darum, schöne Dokumente zu erstellen, sondern darum, Ihren Geschäftsbetrieb zu verbessern.

Um daher den größten Nutzen aus Richtlinien, Verfahren, Plänen und anderen Dokumenten zu ziehen, müssen Sie eine Balance halten – erstellen Sie nur jene Dokumente, die Ihnen wirklich helfen, die Art und Weise, wie Sie Dinge tun, zu verbessern, aber übertreiben Sie es nicht – die Dokumentation ist nicht reiner Selbstzweck.

Aus der Sicht von ISO-Standards hat die Dokumentation zumindest zwei wichtige Rollen: interne Regeln zu definieren, die für Unternehmen als Tool zur Verbesserung ihres Betriebs agieren und Auditoren zu helfen herauszufinden, ob ein Unternehmen wirklich dem Standard entspricht. Dies ist der Grund, warum ISO-Standards ziemlichen Nachdruck auf die Dokumentation legen – sie spezifizieren, welche Dokumente

obligatorisch sind und, in manchen Fällen, was der Inhalt eines bestimmten Dokuments sein sollte.

ISO-Standards gehen sogar noch einen Schritt weiter – sie definieren, wie die verschiedenen Prozesse und Aktivitäten (und deren Dokumente) zusammenpassen und definieren dadurch, wie ein Managementsystem zu gestalten ist. Und, wie ich zuvor erwähnte – die Dokumente zu haben, bedeutet nicht, dass Sie ein Managementsystem haben, doch ohne Dokumente wäre Ihr Managementsystem nicht möglich.

1.2 Wer sollte dieses Buch lesen?

Dieses Buch ist in erster Linie für Anfänger auf diesem Gebiet und für Leute mit moderatem Wissen über die ISO-Dokumentation geschrieben – ich strukturierte dieses Buch so, dass jemand mit keinerlei vorheriger Erfahrung oder Kenntnis der ISO-Standards schnell verstehen kann, wie Dokumente und Aufzeichnungen im Kontext von ISO-Standards zu handhaben sind. Wenn Sie hingegen bereits Erfahrung mit der ISO-Dokumentation haben, aber spüren, dass Sie noch Wissenslücken haben, werden Sie dieses Buch ebenfalls hilfreich finden.

Dieses Buch bietet Beispiele der Handhabung von Richtlinien, Verfahren, Plänen und anderen Dokumenten in kleineren und mittelgroßen Organisationen (d.h. Unternehmen mit bis zu 500 Mitarbeitern). Alle hier beschriebenen Prinzipien sind auch für größere Organisationen anwendbar, Sie werden daher dieses Buch auch nützlich finden, wenn Sie für ein größeres Unternehmen arbeiten. Seien Sie sich jedoch bewusst, dass die Lösungen in manchen Fällen komplexer sein müssen, als die in diesem Buch beschriebenen.

Dieses Buch wurde nicht als Anleitung für die Durchführung des Audits geschrieben, kann aber für interne Auditoren, oder sogar Zertifizierungsauditoren, zweckdienlich sein, da es ihnen hilft, alle Anforderungen des Standards zu verstehen und auch die besten Praktiken für die Erstellung der Dokumentation präsentiert – das ist hilfreich, wenn der Auditor in seinem oder ihrem Audit-Bericht Empfehlungen abgeben muss.

Ich glaube, dieses Buch kann auch ganz hilfreich für Berater sein – nachdem ich selbst Berater bin, habe ich mich bemüht, in diesem Buch den logischsten Weg der Handhabung von Dokumenten aufzuzeigen, Sie werden daher durch aufmerksames Lesen dieses Buches Know-how für Ihre zukünftigen Beratungsaufträge hinzugewinnen.

Wenn Sie also ein Produktionsleiter, Ingenieur, Compliance-Beauftragter, Informationssicherheitsexperte, Leiter einer IT-Abteilung, Vorstand, interner Auditor, Berater oder Projektmanager sind, der mit der Implementierung eines ISO-Standards in einem kleinen oder mittelgroßen Unternehmen beauftragt wurde, ist dieses Buch perfekt für Sie.

1.3 Wie dieses Buch zu lesen ist

Hier sind einige der Features dieses Buches, die es Ihnen leichter machen, es zu lesen und in der Praxis zu verwenden:

- Wenn sich bestimmte Abschnitte dieses Buches auf bestimmte Klauseln in den ISO-Standards beziehen, ist die Standard-Klausel im Titel dieses Abschnitts angeführt.
- Da Kapitel 3 die Dokumentation in Bezug auf bestimmte Klauseln des Standards beschreibt, weisen die meisten der Abschnitte diese Elemente auf:

- Zweck – beschreibt kurz, warum eine solche Klausel existiert und wie sie für das Managementsystem angewendet werden kann.
- Inputs – welche Inputs Sie benötigen, um die Anforderung umzusetzen.
- Optionen – welche Optionen Sie berücksichtigen sollten, wenn Sie die Anforderung umsetzen.
- Entscheidungen – welche Entscheidungen Sie treffen müssen, um voranzukommen.
- Dokumentation – beschreibt, wie die Anforderungen des ISO-Standards zu dokumentieren sind.
- Tipp Dokumentation – fasst kurz die Dokumente zusammen, die Sie für jede Anforderung brauchen.

- Einige Abschnitte enthalten Tipps für kostenlose Tools, welche Ihnen ermöglichen, den Standard auf einfachere Weise zu implementieren.
- Am Ende der Kapitel 2 und 3 finden Sie einen Abschnitt mit dem Titel "Erfolgsfaktoren", der hervorhebt, worauf Sie sich konzentrieren müssen.
- Am Ende des Buches, in Kapitel 4, finden Sie eine kürzere Fallstudie, welche erklärt, wie Probleme mit der Dokumentation in realen Situationen gelöst werden können.
- Eine Menge nützlicher Informationen finden Sie in den Anhängen – Glossar, Checklisten für obligatorische Dokumentationen der hauptsächlichen ISO-Standards und die Dokumentationsstruktur für ISO 27001 Anhang A.

1.4 Was dieses Buch nicht ist

Dieses Buch ist fokussiert darauf, wie die Dokumentation für ISO-Standards zu handhaben ist, erklärt jedoch nicht, wie der Standard zu implementieren ist – in Abschnitt 1.5 finden Sie einen Link zu kostenlosem Online-Training, das die gesamte Implementierung erklären wird.

Dieses Buch stellt Ihnen keine fertigen Vorlagen für alle Ihre Richtlinien, Verfahren und Pläne zur Verfügung, es erklärt Ihnen jedoch, wie Sie Ihr Unternehmen auf die Erstellung der Dokumente, die Sie wirklich brauchen, sowie die Dokumente, die zwar nützlich, aber für Ihr Unternehmen keine Verpflichtung sind, vorbereiten. Es wird jedoch nicht erklärt, wie jedes einzelne Dokument im Detail zu schreiben ist. Im Anhang A finden Sie eine Liste obligatorischer Dokumente für jeden wesentlichen ISO-Standard und ebenso eine Liste nicht-obligatorischer Dokumente, die häufig verwendet werden.

Dieses Buch ist keine Kopie irgendeines 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 (da der Standard eher unfreundlich geschrieben ist) und welche Art von Compliance der Auditor zu sehen erwartet.

Begehen Sie daher bitte nicht den Fehler, die Implementierung zu beginnen und Dokumente zu erstellen, ehe Sie den Standard tatsächlich gelesen haben – ich glaube, Sie werden dieses Buch und den ISO-Standard als perfekte Kombination für Ihre zukünftige Arbeit sehen. Den Standard können Sie auf der offiziellen ISO-Website kaufen.

1.5 Zusätzliche Ressourcen

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

- ISO Online-Kurse – kostenlose Online-Schulungen, in denen Sie die Grundlagen von ISO 9001, ISO 14001 und ISO 27001 lernen, einschließlich Tipps, wie die Dokumentation zu erstellen ist
- ISO 27001 kostenlose Downloads, ISO 9001 kostenlose Downloads und ISO 14001 kostenlose Downloads – eine Sammlung von Weißpapieren, Checklisten, Diagrammen, Vorlagen, etc.
- Conformio – Cloud-basiertes Dokumentenmanagementsystem (DMS) und Projektmanagement-Tool, fokussiert auf ISO-Standards.
- ISO 9001 Dokumentations-Toolkit – ein Set aller Dokumentationsvorlagen, die für ISO 9001 erforderlich sind, mit eingeschlossener Experten-Unterstützung, die Sie Schritt für Schritt in Richtung Zertifizierung führt; ähnliche Toolkits gibt es für andere ISO-Standards.
- Offizielle ISO-Website – hier können Sie eine offizielle Version jedes ISO-Standards kaufen.

2
VORBEREITUNG ZUR ERSTELLUNG DER DOKUMENTE

Einer der häufigsten Gründe für das Fehlschlagen von ISO-Projekten ist, dass sich Unternehmen in solche Projekte ohne richtige Vorbereitung gestürzt haben. Und, Teil dieser Vorbereitung, ist zu entscheiden, was mit der Dokumentation zu tun ist.

Hier ist daher, was Sie vorab überlegen müssen:

2.1 Drei Optionen für die Implementierung des Standards und die Erstellung der Dokumentation

Ganz am Anfang der ISO-Implementierung sind Sie wahrscheinlich von den vielen Ansätzen, wie man ein solches Projekt erfolgreich beginnt und abschließt, überfordert. Meines Erachtens gibt es drei grundsätzliche Optionen für die Implementierung dieser Standards und die Erstellung der notwendigen Dokumente: (1) man macht es komplett unter Verwendung der eigenen Mitarbeiter, (2) man verwendet einen Berater, oder (3) (irgendwie in der Mitte) man implementiert den Standard im „Do-it-yourself"-Verfahren und macht sich externes Know-how zu Nutze.

Jedoch sind diese Vorgehensweisen nicht für jedermann anwendbar – hier ist eine Erklärung von jeder dieser Optionen und für welche Situationen sie sich eignen.

1) Implementierung des Standards unter Verwendung Ihrer eigenen Mitarbeiter. Das ist, wenn Sie entscheiden, den Standard ohne externe Hilfe zu implementieren und nur die Kenntnisse und die Kapazität Ihrer eigenen Mitarbeiter zu nutzen. Bei dieser Option machen Ihre Mitarbeiter alle Analysen, führen die Interviews durch, erstellen die Dokumentation, etc.

Vorteile. Das ist die wahrscheinlich billigste Option, da Sie nicht für externe Dienstleistungen bezahlen. Sie gestatten auch niemandem von außerhalb, etwas über Ihre internen Prozesse oder Ihre Dokumentation zu erfahren. Und schließlich erhöht das Schreiben ihrer eigenen Dokumentation das Engagement Ihrer Mitarbeiter hinsichtlich der erforderlichen Veränderungen.

Nachteile. Das ist wahrscheinlich die langsamste Option, da Sie alles selbst machen. Wenn Ihre Mitarbeiter nicht erfahren oder kompetent genug sind, könnte sich das aufgrund der Fehler, die sie machen könnten, als die teuerste Option herausstellen.

2) Verwendung eines Beraters. Bei dieser Option heuern Sie einen Experten von außerhalb an (für gewöhnlich ist das ein lokaler Berater), der Erfahrung mit der Implementierung des Standards hat – diese Person nimmt dann die Analyse Ihres Unternehmens vor, führt die Interviews, schreibt die Dokumentation, und alles andere – im Grunde genommen implementiert sie den gesamten Standard in Ihrem Namen.

Vorteile. Das ist definitiv der schnellste Weg, den Standard zu implementieren – wenn Sie einen guten Berater anstellen, wird er oder sie eine Menge Erfahrung haben und wissen, wie das Projekt zu organisieren ist, um es schnell abzuschließen. Das ist auch der beste Weg, wenn Ihre Mitarbeiter überhaupt keine Zeit haben, um sich dem Projekt zu widmen. Auch wenn Dinge verändert werden müssen, könnte das Management jemandem von außerhalb des Unternehmens mehr vertrauen.

Nachteile. Berater kosten natürlich Geld, daher ist das die teuerste Option. Darüber hinaus öffnen Sie einem Außenstehenden den Zugang zu fast allen Ihren Betriebsgeheimnissen (z.B. wie das Unternehmen organisiert ist, seine Hauptprozesse und entscheidenden Wettbewerbsvorteile, wer die wichtigsten Leute sind, etc.). Und schließlich könnten die Mitarbeiter, wenn jemand von außerhalb die Dokumentation erstellt, das Gefühl haben, dass ihnen diese Richtlinien und Verfahren aufgezwungen werden und könnten daher oft nach Wegen suchen, diese zu umgehen. Außerdem – wenn sich der Berater verabschiedet hat, können die Mitarbeiter sehr oft die Dokumentation nicht pflegen, weil sie sich nicht das gesamte notwendige Wissen aneigneten.

3) Implementierung des Standards im DIY-Verfahren und Nutzung von externem Know-how. Diese Option wurde in den letzten paar Jahren sehr beliebt und ist im Grunde genommen etwas, das zwischen den ersten beiden Optionen liegt. Das ist, wenn Ihre Mitarbeiter die gesamte Implementierung machen, jedoch Know-how, Dokumentation und Unterstützung von einer externen Partei erhalten.

Vorteile. Diese Option ist nicht so teuer wie ein Berater und dennoch erhalten Sie alles an notwendigem Know-how und Unterstützung. Darüber hinaus eröffnen Sie niemandem von außerhalb den Zugang zu Ihren vertraulichen Informationen. Da Ihre Mitarbeiter außerdem die Dokumentation selbst schreiben, wird deren Engagement zur Einhaltung der neuen Regeln wahrscheinlich viel größer sein.

Nachteile. Ihre Mitarbeiter müssen dennoch alles über die Implementierung lernen, daher ist das nicht der schnellste Weg, den Standard zu implementieren. Auch löst diese Option nicht das Problem, wenn Ihre Mitarbeiter mit anderen Projekten komplett überlastet sind und absolut keine Zeit für etwas Neues haben.

Welche Option sollte man also wählen? Sie sollten den Standard unter Verwendung Ihrer eigenen Mitarbeiter implementieren, wenn Sie Mitarbeiter haben, die bereits Erfahrung mit der Implementierung haben, wenn Sie sehr vertrauliche Daten haben und wenn Ihr Budget sehr niedrig ist. Andererseits, wenn Sie es eilig haben und nicht befürchten müssen, dass Betriebsgeheimnisse offengelegt werden, dann sollten Sie einen Berater verwenden; natürlich benötigen Sie für diese Option ein gutes Budget. Die „Do-it-yourself"-Implementierungsoption sollten Sie wählen, wenn Sie möchten, dass Ihre Mitarbeiter lernen, wie es getan wird, wenn Sie nicht zu sehr in Eile sind und wenn Ihr Projektmanager ein paar Stunden pro Tag für dieses Projekt aufwenden kann; und natürlich, wenn Ihr Budget nicht allzu hoch ist.

2.2 Reihenfolge der Erstellung der Dokumentation & Zusammenhang mit dem PDCA-Zyklus

Die gute Nachricht ist: die ISO-Standards haben es für Sie leichter gemacht, sie zu implementieren und die Dokumentation zu erstellen, indem sie Ihnen Implementationsschritte beistellen.

Alle mit Anhang SL konformen Standards (z.B. ISO 9001, ISO 14001, ISO 27001, ISO 22301) sind aufklare und sequentielle Art und Weise geschrieben, daher sollte Ihre Implementierung im Grunde genommen fast exakt der gleichen Reihenfolge folgen, in der der Standard geschrieben ist. Oder, genauer gesagt, sollten Ihre Schritte im Projektplan in der Reihenfolge, in der sie geschrieben sind, den Klauseln 4 bis 10 dieser Standards gleichen.

Natürlich werden die Ergebnisse der meisten dieser Schritte in der Implementierung verschiedene Dokumente sein – Sie werden alle obligatorischen Dokumente abdecken müssen, plus

alle Dokumente, die Sie als notwendig für Ihr Unternehmen erachten. Listen der obligatorischen Dokumente finden Sie in den Anhängen dieses Buches und in Abschnitt 3.4 erkläre ich, wie man die nicht-obligatorischen Dokumente wählt, die zu erstellen sind.

Diese Sequentialität ist die Konsequenz des, entsprechend des sogenannten Plan-Do-Check-Act(PDCA)-Zyklus geschriebenen, Standards, was aussagt, dass man, um ein effektives Managementsystem zu haben, zuerst einen *Plan* braucht, was man vorhat zu tun (einschließlich dem Setzen von Zielen), dann muss man implementieren (*Do*-Phase), was man geplant hat, danach kommt ein *Check*, ob die Implementierung die geplanten Ergebnisse erzielte und schließlich müssen die Lücken gefüllt werden (*Act*-Phase) zwischen dem, was erreicht wurde und dem, was ursprünglich geplant wurde. Da die Klauseln 4 bis 10 genau diese Logik verfolgen, ist dies der Grund, warum man dieser Logik ebenfalls folgen sollte.

Beachten Sie bitte, dass ich, wenn ich das Wort *Implementierung* in diesem Buch verwende, nicht unbedingt nur die Implementierungs(Do)-Phase im PDCA-Zyklus meine – mit *Implementierung* meine ich alle Schritte, die notwendig sind, um alle Anforderungen eines bestimmten Standards umzusetzen, egal, zu welcher Phase des PDCA-Zyklus sie gehören.

Tipp kostenloses Tool: Conformio ist ein Online-Tool, das alle Schritte in der ISO 9001-, ISO 14001- und ISO 27001-Implementierung abdeckt und auch Leitfäden für jeden der Implementierungsschritte beinhaltet.

2.3 Verwendung von Tools und Vorlagen

Wenn Sie beginnen, ein komplexes Rahmenwerk wie ISO-Standards zu implementieren, suchen Sie vermutlich nach einem

Weg, Ihren Job einfacher zu machen. Wer würde das nicht? Schließlich klingt es nicht nach einem sehr interessanten Job, das Rad neu zu erfinden.

Doch Vorsicht, wenn Sie mit der Suche nach solchen Tools beginnen – nicht jedes Tool hilft Ihnen: Sie könnten mit einem LKW-Rad enden, das nicht auf das Auto, das Sie fahren, passt.

Arten von Tools. Lassen Sie uns zuerst damit beginnen, welche Arten von Tools Sie im Markt finden werden, die speziell für ISO-Standards gemacht sind:

a) Automatisierungstools – diese Tools helfen Ihnen, einen Teil Ihrer Prozesse halb zu automatisieren – z.B. Management des Projekts, Durchführung der Risikobewertung, Speicherung und Genehmigung der Dokumentation, Management von Vorfällen, Unterstützung bei der Messung, etc.

b) Tools für die Erstellung der Dokumentation – diese Tools helfen Ihnen, Richtlinien und Verfahren zu entwickeln – für gewöhnlich enthalten Sie Vorlagen, Tutorials für die Erstellung der Dokumentation, etc.

Vor- und Nachteile von Automatisierungstools. Die Grundidee von Automatisierungstools ist, zeitaufwändige Aktivitäten, wie die Verwendung von Tabellenblättern für die Risikobewertung in einigen Ihrer Abteilungen, zu eliminieren – ein cleveres Tool hilft Ihnen, diese Ergebnisse zusammenzuführen. Automatisierungstools sollten Ihnen auch helfen, das gesamte ISO-Projekt abzuwickeln, indem sie vorschlagen, welche Schritte Sie ergreifen müssen, wer wofür verantwortlich ist, welche Dokumente zu produzieren und zu genehmigen sind, von wem, etc.

Das größte Problem mit Automatisierungstools ist, dass die meisten davon für größere Unternehmen gemacht sind: der

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

LITERATURVERZEICHNIS

ISO 9001:2015, Quality management systems – Requirements, International Standardization Organization, 2015

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

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

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

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

OHSAS 18001:2007, Occupational health and safety management systems – Requirements, BSI, 2007

Kosutic, Dejan, *Becoming Resilient*, Zagreb: EPPS Services Ltd, 2013

Kosutic, Dejan, *Secure & Simple*, Zagreb: Advisera Expert Solutions Ltd, 2016

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

http://training.advisera.com/course/iso-27001-foundations-course/ *ISO 27001 Foundations Course*, Advisera.com

INDEX

Management der ISO-Dokumentation: Ein leicht verständlicher deutscher Leitfaden

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

Denken und agieren Sie wie ein Berater mit dieser praktischen Anleitung für das Management der ISO-Dokumentation.

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

- ✓ die Reihenfolge der Erstellung der Dokumentation
- ✓ wie man sich für eine Dokumentationsstrategie entscheidet
- ✓ ob Sie Tools und Vorlagen nutzen sollten
- ✓ wie Dokumente und Aufzeichnungen zu lenken sind
- ✓ welche die obligatorischen Dokumente sind
- ✓ wie man entscheidet, welche nicht-obligatorischen Dokumente zu erstellen sind
- ✓ wie man Dokumente erstellt, die von Ihren Kollegen akzeptiert werden
- ✓ all das, und noch viel mehr…

Geschrieben in leicht verständlicher Sprache, ist *Management der ISO-Dokumentation: Ein leicht verständlicher deutscher Leitfaden* für Leute erstellt, die zum ersten Mal ISO-Dokumente bearbeiten und eine klare Anleitung benötigen, wie dies zu tun ist. Ob Sie nun ein erfahrener ISO-Praktiker oder ein Neuling auf diesem Gebiet sind, es ist das einzige Buch, das Sie jemals zu diesem Thema benötigen werden.