VORBEREITUNGEN FÜR EIN ISO-IMPLEMENTIERUNGSPROJEKT: EIN LEICHT VERSTÄNDLICHER DEUTSCHER LEITFADEN

ISO TASCHENBUCH SERIE

05

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

DEJAN KOSUTIC

Vorbereitungen für ein ISO-Implementierungsprojekt: 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

Management der ISO-Dokumentation: Ein leicht verständlicher deutscher Leitfaden

Dejan Kosutic

Vorbereitungen für ein ISO-Implementierungsprojekt: 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: 978-953-8155-12-3

Erstauflage, 2017

Originaltitel: Preparations for an ISO Implementation Project: 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

ABBILDUNGSVERZEICHNIS

VORWORT

Als wir vergangenes Jahr mein Buch *Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own* publizierten, realisierte ich sehr bald, dass viele Leute nach Informationen dazu suchen, was Sie tun müssen, um ihre ISO-Implementierung erfolgreich zu machen.

Aus diesem Grund habe ich dieses kurze Buch, als Teil der Handbuch-Serie, geschrieben, das nur auf das Thema fokussiert ist, wie man sich auf die Implementierung vorbereitet. Dieses Buch konzentriert sich nicht nur auf ISO 27001 – die Vorbereitungen für die Implementierung sind für jeden Standard gleich, 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, *Vorbereitungen für ein ISO-Implementierungsprojekt: 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, die sich mit den Implementierungsvorbereitungen befassen, 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 die Vorbereitungen für die Implementierung 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 ähnliche Bücher 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 die Vorbereitungen für die Implementierung in kleineren Unternehmen fokussiert – deshalb habe ich die Schritte mit Absicht vereinfacht, so dass Ihre Vorbereitungen relativ 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 die Implementierung Ihres ISO-Standards bereit zu machen, selbst, wenn Sie dies das erste Mal tun.

1
EINFÜHRUNG

Was sind die kostspieligsten Fehler, die Sie bei der ISO-Implementierung machen können? Warum ist die Vorbereitung auf ein ISO-Projekt so wichtig? Und, ist dieses Buch die richtige Wahl für Sie?

Dieses Buch behandelt die Vorbereitungen für jeden ISO-Managementstandard - – 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 im Buch auf „ISO-Standard", oder einfach „Standard", um jeden dieser Standards abzudecken.

Auch verwende ich anstatt z.B. „QMS" für Qualitätsmanagementsystem, oder „ISMS" für Informationssicherheitssystem, einfach den Ausdruck „Managementsystem".

1.1 Die fünf häufigsten Mythen im Zusammenhang mit ISO-Standards / Warum Vorbereitungen nötig sind

In Bezug auf ISO-Standards gibt es viele Missverständnisse, die sehr oft nicht zulassen, dass der Standard als seriöser Kandidat in Betracht kommt, geschweige denn die tatsächliche Implementierung. Eigentlich könnte man diese Mythen als den größten Feind der ISO-Standards bezeichnen.

Hier einiges, das ich nur zu oft höre:

"Wir lassen es den Administrator erledigen."

Das ist der Favorit des Managements – „Wir übergeben dieses ISO-Projekt an diesen Administrator, er kostet uns jedenfalls nicht zu viel." Das Problem mit diesem Ansatz ist nur, dass das Projekt niemals enden wird – weil der Administrator nicht genug Wissen für diese Art von Projekten hat, wahrscheinlich nicht genug Zeit hat und sicherlich nicht über die ausreichenden Befugnisse verfügt.

"Wir werden das in ein paar Wochen implementieren"

Sie könnten Ihren ISO-Standard in zwei oder drei Wochen implementieren, doch wird es nicht funktionieren – Sie hätten nur einen Haufen Richtlinien und Verfahren, um die sich niemand schert. Die Implementierung eines Managementsystems bedeutet, dass Sie Änderungen umsetzen müssen und es braucht Zeit, bis Änderungen von Ihren Mitarbeitern akzeptiert werden.

Ganz zu schweigen davon, dass Sie nur jene Kontrollen oder Prozesse implementieren müssen, die tatsächlich gebraucht werden und die Analyse davon, was wirklich gebraucht wird, braucht ebenfalls Zeit.

"In diesem Standard geht es nur um Dokumentation"

Die Dokumentation ist ein wichtiger Teil der Implementierung eines ISO-Standards, doch endet es nicht mit der Dokumentation. Schwerpunkt einer ISO-Implementierung ist, dass die Mitarbeiter Ihre Aktivitäten auf definierte Art und Weise durchführen und die Dokumentation ist dazu da, Ihnen dabei zu helfen. Auch die Aufzeichnungen, die produziert werden, werden Ihnen helfen, zu messen, ob Sie die Ziele, die Sie sich für das Managementsystem gesetzt haben, erreicht werden und Ihnen ermöglichen, jene Aktivitäten, welche die Erwartungen nicht erfüllen, zu korrigieren.

Sie könnten daher die Dokumentation als ein Tool zur Handhabung von z.B. Ihrer Qualität für ISO 9001, Umwelt für ISO 14001 oder Sicherheit für ISO 27001 betrachten, anstatt sie als Overkill für Ihren Betrieb zu sehen.

"Der einzige Vorteil des Standards sind die Marketing-Zwecke"

"Wir tun dies nur, um das Zertifikat zu bekommen, nicht wahr?" Das ist (leider) die Art und Weise, in der 80 Prozent der Unternehmen denken. Ich versuche hier nicht zu argumentieren, dass der ISO-Standard nicht zu Werbe- und Verkaufszwecken genutzt werden sollte, doch können Sie auch weitere sehr wichtige Vorteile damit erzielen – die Hauptvorteile sind in Abschnitt 2.1 aufgelistet.

"Wir brauchen ein GRC-Tool, um den ISO-Standard zu implementieren"

"Governance, Risk & Compliance"-Tools können tatsächlich sehr hilfreich sein, allerdings sind sie für die ISO-Implementierung beileibe nicht erforderlich. Sie können Ihre gesamte Dokumentation auf Ihrem vorhandenen Server, oder in einem Cloud-Service, wie Dropbox, oder auf Ihrem Computer unterbringen; automatische Logs sollten auf jenen Systemen gehalten werden, welche sie erstellten – detailliertere Anleitungen finden Sie in Abschnitt 3.9.

Was ich sagen will, ist das Folgende – gehen Sie dieses Buch durch und sehen Sie, was wirklich gebraucht wird und was nicht, und entscheiden Sie dann, wofür Sie das meiste Ihrer Zeit und Ihres Geldes in Bezug auf Ihr ISO-Projekte aufwenden möchten.

Der Hauptgedanke dieses Buches ist, Ihnen zu helfen, kostspielige Fehler zu vermeiden – mit anderen Worten, sich auf Ihr ISO-Projekt vorzubereiten anstatt sich übereilt hineinzustürzen.

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-Implementierung geschrieben – ich strukturierte dieses Buch so, dass jemand mit keinerlei vorherigen Erfahrung oder Kenntnissen von ISO-Standards schnell verstehen kann, wie man sich auf ein Implementierungsprojekt vorbereitet. Wenn Sie aber bereits Erfahrung mit der ISO-Implementierung haben, jedoch spüren, dass Sie noch Wissenslücken haben, werden Sie dieses Buch ebenfalls als hilfreich betrachten.

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

Dieses Buch bietet Beispiele der Vorbereitungen für die Implementierung von ISO-Standards in kleineren und mittelgroßen Organisationen (d.h. Unternehmen mit bis zu 500 Mitarbeitern). Alle hier beschriebenen Prinzipien sind auch für größere Organisationen anwendbar, wenn Sie also für ein größeres Unternehmen arbeiten, könnten Sie dieses Buch ebenfalls nützlich finden; sind Sie sich jedoch bitte bewusst, dass in manchen Fällen die Lösungen etwas komplexer als die hier beschriebenen zu sein haben werden – Sie könnten, zum Beispiel, eine komplexere Projektmanagement-Struktur als die in Abschnitt 3.5, Errichtung einer Projektmanagement-Struktur, vorgeschlagene Struktur haben wollen.

Zusammenfassend kann gesagt werden, dass dieses Buch Ihnen ein systematisches Bild der Aktivitäten, die Sie durchführen müssen, und der Entscheidungen, die Sie treffen müssen, gibt, ehe Sie mit der Implementierung Ihres ISO-Standards beginnen - durch die Verwendung dieses Buches stellen Sie sicher, dass Sie nicht bereits ganz am Anfang kostspielige Fehler begehen.

1.3 Was dieses Buch nicht ist

Dieses Buch ist auf die Aktivitäten und Entscheidungen, die Sie vor dem Start Ihres ISO-Implementierungsprojekts in Betracht ziehen müssen, fokussiert, es erklärt jedoch nicht die eigentliche Implementierung eines bestimmten ISO-Standards. (Im nächsten Abschnitt finden Sie Verweise auf Materialien, die Ihnen bei der Implementierung helfen werden.)

Dieses Buch bietet Ihnen keine fertigen Vorlagen für alle Ihre Richtlinien, Verfahren und Pläne, Sie finden jedoch in den Anhängen dieses Buches eine Reihe von Vorlagen, zum Beispiel für den Projektplan.

Dieses Buch ist keine Kopie irgendeines ISO-Standards – Sie können das Lesen des Standards nicht durch das Lesen dieses Buches ersetzen. Machen Sie daher bitte nicht den Fehler, die Implementierung eines Standards zu starten, ohne diesen tatsächlich gelesen zu haben - ich glaube, Sie werden dieses Buch und den ISO-Standard als perfekte Kombination für Ihre zukünftige Arbeit sehen. Kaufen können Sie den Standard auf der offiziellen ISO-Website.

1.4 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 lernen, wie ISO 9001, ISO 14001 und ISO 27001 zu implementieren sind, einschließlich von Tipps dazu, wie man sich für die Zertifizierung entscheidet.
- ISO 27001 kostenlose Downloads, ISO 9001 kostenlose Downloads, ISO 14001 kostenlose Downloads, OHSAS 18001 kostenlose Downloads und ISO 20000 kostenlose Downloads – eine Sammlung von Weißpapieren, Checklisten, Diagrammen, Vorlagen, etc.
- Conformio – ein 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, welche Sie Schritt für Schritt durch die Implementierung führt; ähnliche Toolkits existieren auch für andere ISO-Standards.
- Offizielle ISO-Website – hier können Sie eine offizielle Version von jedem ISO-Standard erwerben.

2
DIE UNTERSTÜTZUNG IHRES MANAGEMENTS UND ANDERER MITARBEITER GEWINNEN

Es gibt in Wirklichkeit einen, für das Scheitern ihrer Projekte verantwortlichen Hauptgrund, den die meisten ISO-Praktiker betonen: fehlendes Verständnis seitens des Topmanagements, und demzufolge dessen fehlende kontinuierliche Unterstützung.

Das Topmanagement ist jedoch nicht das einzige Problem. Sehr oft werden ISO-Praktiker, wenn schon nicht komplett missverstanden, dann zumindest gemieden von den anderen Mitarbeitern im Unternehmen. Mit „ISO-Praktiker" meine ich jemanden, der für die Implementierung eines bestimmten ISO-Standards verantwortlich ist.

Die Lösung zu diesem Problem? Das wird Ihnen wahrscheinlich nicht gefallen: Sie müssen eine Mischung aus Diplomat und Verkäufer werden. Sie werden die Idee des Standards, an dem Sie arbeiten, Ihrem Management, Ihren Mitarbeitern und Ihren Partnern verkaufen müssen und werden all Ihre Überzeugungskraft anwenden müssen, um sie zu überzeugen. Und nein, bei Ihrem Job als ISO-Praktiker geht es nicht nur um Richtlinien und Verfahren – es geht vor allem um Psychologie und das Überzeugen von Leuten rund um Sie.

Dieses Kapitel zeigt Ihnen, wie das getan wird.

2.1 Wie Sie Ihr Topmanagement überzeugen, den ISO-Standard zu implementieren

Wenn Sie glauben, Ihr Management hört sich gerne Ihre großartigen Ideen zu einer neuen Richtlinie oder einer neuen Technologie an, dann liegen Sie falsch – es ist ihnen einfach egal.

Was das Management hören möchte (und auch versteht), sind Profite, Marktanteile, Kundenzufriedenheit, Kosteneinsparungen, Unternehmensstrategien und Unternehmensrisiken. Und Sie können es ihnen nicht verübeln – es ist schließlich das, worum es in deren Jobs geht.

Wenn Sie sie also nicht ändern können, müssen Sie sich selbst ändern. Wenn Sie von Anfang an möchten, dass sie Ihnen zuhören, müssen Sie die Sprache sprechen, die sie verstehen – und sie werden sie nur verstehen, wenn Sie ihnen die wirtschaftlichen Vorteile der Implementierung Ihres Standards darlegen.

Nach meiner Erfahrung gibt es vier potentielle Vorteile, die Sie betrachten sollten:

1. Compliance. Es gibt in fast jedem Land immer mehr Gesetze und Bestimmungen, denen durch die Implementierung eines bestimmten Standards entsprochen werden kann (z.B. kann der Schutz persönlicher Daten, der Schutz staatlicher Verschlusssachen durch die Implementierung von ISO 27001 bewältigt werden). Was jedoch noch interessanter ist, ist, dass es eine zunehmende Zahl von Geschäftskunden gibt, die von ihren Lieferanten verlangen, einen bestimmten Standard zu implementierten (z.B. ein Bauunternehmen, das von

seinen Lieferanten verlangt, ISO 9001-zertifiziert zu sein). Die gute Nachricht ist, dass ISO-Standards einen perfekten Rahmen für die Einhaltung aller dieser Anforderungen abgeben, zum Teil deswegen, weil diese internationalen Standards bei der Entwicklung dieser Gesetze und Bestimmungen als Modell dienten. Das bedeutet: weniger Mühe im Compliance-Prozess und weniger zu bezahlende Strafen.

2. Marketing-Vorteil. Verfügt Ihr Unternehmen über das ISO-Zertifikat und Ihre Mitbewerber nicht, könnten Sie sogar neue Kunden gewinnen, weil es Ihnen möglich ist, potentielle Kunden davon zu überzeugen, dass Sie in irgendeiner Form eine Leistung erbringen können (z.B. besseres Handling von Kundenanforderungen mit ISO 9001, höhere Belastbarkeit mit ISO 22301, etc.), welche Ihre Mitbewerber nicht bieten können. Das bedeutet: ein erhöhter Marktanteil und höhere Gewinne.

3. Senkung der Kosten. ISO-Standards werden für gewöhnlich als Kosten ohne offensichtlichen finanziellen Gewinn angesehen. Es gibt jedoch einen finanziellen Gewinn, wenn Sie Ihre Kosten senken, die z.B. durch Störfälle oder Kundenbeschwerden verursacht werden. (Wahrscheinlich haben Sie irgendeine Art von Vorfällen im Zusammenhang mit Sicherheit, Arbeitsschutz, Umwelt oder anderen Störungen; wahrscheinlich haben Sie auch Kundenbeschwerden – alles davon kostet Sie Geld.) Es stimmt, dass es schwierig ist, zu berechnen, wie viel Geld Sie sparen könnten, wenn Sie solche Vorfälle/Beschwerden verhinderten – doch klingt es immer gut, wenn Sie dem Management solche Fälle aufzeigen. (Später in diesem Kapitel – in Abschnitt 2.3 – werde ich erklären, wie man die Einsparungen für Informationssicherheitsvorfälle kalkuliert.)

4. Optimierung der Geschäftsprozesse. Dies ist wahrscheinlich das am meisten Unterschätzte – wenn Sie ein Unternehmen sind, das in den letzten paar Jahren deutlich gewachsen ist, könnten Sie Probleme haben, wie – wer hat was zu entscheiden, wer berichtet an wen, wer ist verantwortlich für was, etc. ISO-Standards sind im Aussortieren dieser Dinge besonders gut – sie zwingen Sie, sehr genaue Rollen und Verantwortlichkeiten zu definieren und stärken damit Ihre interne Organisation.

Ich will damit nicht sagen, dass jeder dieser vier Vorteile für Ihre Organisation zutreffend ist, doch besteht die Chance, dass Sie zumindest zwei finden werden, die für Ihre Organisation wirklich relevant sind. Und, Sie müssen sich mit Ihren Kollegen im Unternehmen beraten, weil Sie letztlich herausfinden müssen, welcher dieser Vorteile für Ihr Topmanagement am interessantesten ist und welcher Ihre Unternehmensstrategie unterstützt. Der beste Weg, dies zu tun, wäre ein Brainstorming zu diesen Vorteilen mit Ihren Kollegen von der kaufmännischen Seite Ihrer Organisation, sowie mit jenen in Leitungsfunktionen.

Natürlich müssen Sie auch Wege finden, um Ihr ISO-Projekt mit der Unternehmensstrategie zu verknüpfen. Hier ist ein Beispiel: angenommen, Ihr Unternehmen möchte damit beginnen, Cloud-Services anzubieten, was bedeutet, dass sensible Daten Ihrer Kunden geschützt werden müssen; wenn Sie ISO 27001 implementieren, wird dies nicht nur die Wahrscheinlichkeit für ein Datenleck verringern, sondern auch eine Nichtverfügbarkeit der Services – und so wird ein solches Projekt den von Ihrem Unternehmen beschlossenen strategischen Schritt unterstützen.

Sehen Sie sich bitte auch die Mini-Fallstudie im Kapitel 4 an: Gewinn des Engagements des Topmanagements in einem Staatsunternehmen.

Der nächste Schritt ist, herauszufinden, wie etwas in den Köpfen Ihres Managements bewirkt werden kann.

2.2 Wie Sie die Vorteile Ihrem Topmanagement präsentieren

Erwarten Sie nicht, dass Ihr Management alle Vorteile nach einem 20 Minuten-Meeting erfasst, ganz gleich, wie nett Ihre PowerPoint-Präsentation aussieht. Es wird für Ihr Management Zeit brauchen, zu verstehen.

Hier sind einige Techniken, die Sie für die effektivere Präsentation Ihrer Sache anwenden können:

"Elevator Speech". Es besteht die Chance, dass Sie bei informeller Gelegenheit mehr erreichen als in formellen Meetings – z.B. wenn Sie zufällig in einer Cafeteria auf Ihren CEO stoßen, in einem Aufzug, oder Ähnlichem. Sind Sie auf so eine Gelegenheit nicht vorbereitet, werden Sie wahrscheinlich verwirrt sein – deshalb müssen Sie einen sogenannten „Elevator Speech", eine 30 bis 60 Sekunden lange Rede, in der Sie Ihre Sache anschaulich vortragen, vorbereiten. Wenn Sie es gut einüben, werden Sie sicher und überzeugend klingen. Mein „Elevator Speech", zum Beispiel, (als Berater, der versucht seine Services zu verkaufen), ist wie folgt: *Die Investition in ISO 27001 wird sich bezahlt machen, wenn man nur einen einzigen Störfall mittlerer Größe verhindert, ganz zu schweigen von großen Störfällen.*

Finden Sie einen Verbündeten. Sie müssen Leute finden, die Ihrem CEO nahestehen und naturgemäß daran interessiert sind, was Sie tun – Ihr Finanzvorstand könnte, zum Beispiel, die Implementierung des ISO-Standards als eine Möglichkeit sehen, das finanzielle Risiko für das Unternehmen zu verringern und könnte sich somit entscheiden, Ihre Bemühungen zu

unterstützen; der Chef der Compliance-Abteilung könnte Ihre Projekt als eine Möglichkeit sehen, ihn von einem Teil seiner Arbeitsbelastung zu entlasten, während die Marketing-Leute dies als weitere wichtige Verkaufsargumente betrachten könnten. Machen Sie auf jeden Fall Ihre Hausaufgaben und erforschen Sie, wer an den im vorigen Abschnitt genannten Vorteilen Interesse haben könnte.

Diese Leute geben Ihnen nicht nur weitere Einsichten darüber, wie ein bestimmter ISO-Standard dem Unternehmen helfen wird, Sie werden es auch einfacher machen, auf die Agenda des Topmanagements zu gelangen.

30-20-10-Regel. Wenn Sie Ihre PowerPoint-Präsentation machen, vergessen Sie alle diese hochtrabenden Statistiken, die Sie gefunden haben und die Hunderten von Folien, die Sie vorbereiteten. Entscheiden Sie sich stattdessen für die 30-20-10-Regel: verwenden Sie Schriftgröße 30, ein Maximum von 20 Minuten, und bis zu 10 Folien. Und konzentrieren Sie sich auf die Vorteile – das ist die hauptsächliche Botschaft, die Sie überbringen müssen. (Siehe auch Anhang G für eine Projektvorschlag-Vorlage.)

Vorsicht mit Begriffen. Denken Sie daran, dass Ihre Zielgruppe Manager sind, die Ihre fachspezifischen Ausdrücke nicht verstehen oder nicht mögen. Zum Beispiel, wenn Sie Informationssicherheit/ISO 27001 präsentieren:

Anstatt:	verwenden Sie das:
Backup, Brandunterdrückungssysteme (und andere Schutzvorkehrungen)	Vorbeugung (*Wir werden vorbeugen…)*
Kosten	Investitionen (*Durch die Investition in …, werden wir*

	xyz Euro sparen…)
Wahrscheinlichkeit	Risiko (*Wir werden das Risiko von … verringern*)
Vorfall	Schaden (*Wir werden den Schaden durch Implementierung von … verringern*)
Desaster	Verlust/Ausfallzeit (*Wir werden einen Verlust von xyz Euro haben; unsere zu erwartende Ausfallzeit wird … betragen*)

Abbildung 1: Zu vermeidende und zu verwendende Wörter bei der Präsentation eines ISO-Projekts

Und vor allem, sind Sie geduldig und beharrlich – verhalten Sie sich wie ein echter Verkäufer. Nach einiger Zeit werden Sie sicher einiges an Fortschritt bemerken – vielleicht nicht in den ersten paar Tagen oder sogar Monaten, doch lassen Sie sich davon nicht entmutigen.

2.3 Beispiel einer Investitionsrendite (ROI) für die Informationssicherheit

Im folgenden Beispiel geht es um die Informationssicherheit; es kann jedoch auf sehr ähnliche Weise auf Umweltereignisse, und vielleicht sogar auf Arbeitsschutz-Vorfälle, angewendet werden.

Sie werden sehr oft gefragt werden: Wenn wir xyz Euro in Ihre Informationssicherheit investieren, wird sich das bezahlt machen? Was ist der ROI?"

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

LITERATURVERZEICHNIS

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

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

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

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

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

ISO/DIS 45001, Occupational health and safety management systems – Requirements with guidance for use, International Organization for Standardization, 2015

ITIL 2011, Axelos, 2011

Kosutic, Dejan, *9 Steps to Cybersecurity*, Zagreb: EPPS Services Ltd, 2012

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

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

https://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

Vorbereitungen für ein ISO-Implementierungsprojekt: Ein leicht verständlicher deutscher Leitfaden

Ein Schritt-für-Schritt-Handbuch für ISO-Praktiker in Kleinunternehmen

Denken und agieren Sie wie ein erfahrener Implementierer mit diesem ausführlichen und praktischen Leitfaden, der Ihnen sagt, welche Vorbereitungen Sie zu treffen haben, bevor Sie Ihr Projekt zur Implementierung von ISO 9001, ISO 14001, ISO 27001, oder eines anderen ISO-Managementstandards beginnen.

Der Autor und erfahrene Berater Dejan Kosutic teilt sein Wissen und seine praktische Erfahrung mit Ihnen in einem unschätzbaren Buch. Sie werden erfahren:

- ✓ Wie man sein Topmanagement überzeugt, den Standard zu implementieren
- ✓ Wie man die Geschäftsvorteile der ISO-Implementierung präsentiert
- ✓ Wie man das Engagement der anderen Mitarbeiter im Unternehmen gewinnt
- ✓ Wie man seine Strategie für die ISO-Implementierung entwickelt – erfahren Sie die 3 Optionen, die Sie haben
- ✓ Wie man einen Berater auswählt
- ✓ Wie man eine Projektmanagement-Struktur einrichtet
- ✓ Wie lange das Projekt dauern wird und wie viel es kosten wird
- ✓ Ob Sie Tools und Vorlagen verwenden sollten
- ✓ All das, und noch viel mehr…

Geschrieben in leicht verständlicher Sprache, ist *Vorbereitungen für ein ISO-Implementierungsprojekt: Ein leicht verständlicher deutscher Leitfaden* für Leute erstellt, die das erste Mal eine ISO-

Implementierung in Angriff nehmen und klare Anleitungen benötigen, was vor dem Projektstart zu tun ist. Ob Sie nun ein erfahrener Praktiker oder ein Neuling auf dem Gebiet sind, es ist das einzige Buch, das Sie jemals zu diesem Thema benötigen werden.