GESTIRE LA DOCUMENTAZIONE ISO: UNA GUIDA IN LINGUAGGIO SEMPLICE

ISO 04

COLLANA LIBRI TASCABILI

Una Guida Passo dopo Passo per Professionisti ISO in Aziende di Piccole Dimensioni

DEJAN KOSUTIC

Gestire la Documentazione ISO: Una Guida in Linguaggio Semplice

Altre opere dell'autore:

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

Prepararsi all'Audit di Certificazione ISO: Una Guida in Linguaggio Semplice

Audit Interno ISO: Una Guida in Linguaggio Semplice

Dejan Kosutic

Gestire la Documentazione ISO: Una Guida in Linguaggio Semplice

Una Guida Passo dopo Passo per Professionisti ISO in Aziende di Piccole Dimensioni

Advisera Expert Solutions Ltd
Zagabria, Croazia

Prima edizione pubblicata da Advisera Expert Solutions Ltd
Zavizanska 12, 10000 Zagabria
Croazia
Unione Europea
http://advisera.com/

ISBN: 978-953-8155-14-7

Prima Edizione, 2017

Titolo originale: "Managing ISO Documentation: A Plain English Guide"

Tradotto dall'inglese da Laura Perreca

L'AUTORE

Dejan Kosutic è autore di numerosi articoli, video tutorial, modelli di documentazione, webinar e corsi sulla ISO 27001, ISO 22301 e altre norme ISO. È l'autore del principale blog su ISO 27001 e ISO 22301 e ha supportato varie organizzazioni, tra cui istituti finanziari, agenzie governative e aziende di IT, nell'implementazione di sistemi di gestione di sicurezza dell'informazione in relazione a queste norme. Ha ottenuto numerosi certificati, tra cui quello di Lead Auditor ISO 27001 e Lead Auditor ISO 9001.

Clicca qui per vedere il suo Profilo LinkedIn.

SOMMARIO

PREFAZIONE

Quando l'anno scorso è stato pubblicato il mio libro *Secure & Simple: A Small-Business Guide to Implementing ISO 27001 On Your Own* ho capito subito che molte persone lo avevano letto principalmente perché erano interessate a imparare come gestire la documentazione.

È per questo motivo che ho realizzato questo libro più breve, parte della collana di manuali, incentrato esclusivamente su argomenti relativi a come gestire le politiche, le procedure, i piani e altri documenti e registrazioni. Questo libro non riguarda esclusivamente la ISO 27001 – le regole per gestire la documentazione sono le stesse per qualsiasi norma - per cui ho adattato questo libro in modo tale che sia perfettamente utilizzabile per le norme ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 22000, OHSAS 18001, ISO 13485 e IATF 16949.

Questo libro, *Gestire la Documentazione ISO: Una Guida in Linguaggio Semplice*, è in realtà un estratto dal libro *Secure & Simple* che ho modificato eliminando soltanto qualche dettaglio. Se lo confronti con le sezioni di *Secure & Simple* che parlano di documentazione, vedrai qui gli stessi paragrafi, con quasi lo stesso testo - come ho accennato, il testo è stato adattato in modo da poter essere letto dal punto di vista di qualsiasi norma ISO.

Allora perché avere due libri che contengono quasi lo stesso testo? Perché ho voluto fornire una lettura veloce alle persone che sono interessate esclusivamente alla gestione della documentazione e non hanno il tempo (o la necessità) di leggere un libro dettagliato sull'implementazione delle norme ISO, ossia un libro come *Secure & Simple*.

Potresti anche essere sconcertato dal fatto che questo libro sia piuttosto breve, mentre esistono sul mercato altre opere sulla documentazione ISO molto più lunghe e dettagliate. È davvero possibile spiegare un argomento così complesso in un libro così breve? Ebbene, ci sono due risposte a questa domanda:

In primo luogo, questo libro è incentrato sulla gestione dei documenti nelle aziende più piccole, pertanto ho intenzionalmente semplificato le descrizioni, in modo che tu possa gestire la documentazione in modo facile, e ho escluso tutti gli elementi necessari solo alle aziende più grandi.

In secondo luogo, e questo è il punto più importante, ho seguito la mia missione aziendale: "Rendiamo le strutture complesse facili da comprendere e semplici da usare". In altre parole, è facile complicare le cose, ma è difficile renderle semplici da capire. Così, quando inizierai a leggere questo libro, noterai che ho eliminato tutti i discorsi difficili da comprendere, tutti i dettagli inutili, e mi sono concentrato esattamente su ciò che deve essere fatto, in un linguaggio comprensibile ai principianti che non hanno avuto precedenti esperienze di implementazione di norme ISO.

Quindi, non ti preoccupare: se hai un'organizzazione di piccole dimensioni, usando questo libro sarai in grado di gestire i documenti in modo ottimale. E vedrai i reali vantaggi di avere documenti adeguati che ti aiutino a svolgere le attività operative all'interno della tua azienda.

1
INTRODUZIONE

Perché hai bisogno di documenti e registrazioni (o "informazioni documentate" come vengono chiamati nelle norme ISO)? Questo libro è la scelta giusta per te?

Questo libro fornisce suggerimenti sulla gestione della documentazione per tutte le norme di gestione ISO: ISO 9001, ISO 14001, ISO 27001, ISO 20000, ISO 13485, ma anche OHSAS 18001 e IATF 16949 (ex ISO / TS 16949), per cui, quando all'interno di questo libro mi riferisco a una "norma ISO" o semplicemente a una "norma", intendo qualunque norma tra quelle sopra elencate.

1.1 Perché la documentazione è importante per i sistemi di gestione ISO?

Forse l'argomento più controverso riguardo alle norme ISO è la documentazione - esistono molte opinioni diverse a riguardo, molto spesso diametralmente opposte:

- "Non abbiamo bisogno di questi documenti, stiamo lavorando benissimo senza: sarebbero solo un inutile sovraccarico".
- "Questa norma si basa tutta sulla documentazione - dobbiamo semplicemente compilare tutti i documenti e otterremo il certificato automaticamente".
- "Dobbiamo scrivere delle politiche e procedure per ogni processo, attività e controllo esistenti nella nostra azienda

- più documenti ci sono, più chiare saranno le regole e più facile sarà per noi essere conformi".

Purtroppo, si sentono molto spesso affermazioni del genere. E, purtroppo, nessuna di esse riflette la vera natura di ciò che le norme ISO richiedono realmente.

Il punto principale dell'implementazione di ogni norma è che i dipendenti eseguano le proprie attività e processi in modo migliore, e la documentazione serve ad aiutare a farlo perché altrimenti questi processi e attività diventerebbero ingestibili. Inoltre, le registrazioni che saranno prodotte ti aiuteranno a verificare se hai raggiunto i tuoi obiettivi e ti permetteranno di correggere quelle attività che risultano meno performanti.

Si potrebbe quindi considerare la documentazione come uno strumento per ottenere una migliore qualità (con la ISO 9001), o sicurezza (con ISO 27001), o protezione ambientale (con la ISO 14001), ecc.: lo scopo è quello di migliorare le attività della tua azienda.

Quindi, per ottenere i maggiori vantaggi da politiche, procedure, piani e altri documenti, è necessario mantenere un equilibrio e scrivere solo i documenti che aiutano veramente a migliorare il modo in cui fai le cose, ma non farti prendere la mano: la documentazione non è un fine in sé.

Dal punto di vista delle norme ISO, la documentazione svolge almeno due ruoli importanti: definire le regole interne che agiranno come strumento per le aziende per migliorare le proprie attività operative e aiutare gli auditor a scoprire se un'azienda è effettivamente conforme allo standard. È per questo motivo che le norme ISO danno una grande enfasi alla documentazione, specificano quali documenti siano obbligatori e, in alcuni casi, quali debbano essere i contenuti di documenti specifici.

Le norme ISO vanno un ulteriore passo avanti: definiscono come i vari processi e le attività (e i relativi documenti) si integrino, e così facendo definiscono come creare un sistema di gestione. E, come accennato in precedenza, avere i documenti non significa che tu abbia un sistema di gestione, ma senza documenti il tuo sistema di gestione non potrebbe esistere.

1.2 Chi dovrebbe leggere questo libro?

Questo libro è scritto principalmente per i principianti in questo campo e per le persone con una conoscenza non approfondita della documentazione ISO - ho strutturato questo libro in modo tale che una persona senza precedenti esperienze o conoscenze sulle norme ISO possa comprendere rapidamente come gestire i documenti e le registrazioni all'interno del contesto delle norme ISO. Tuttavia, se hai esperienza con la documentazione ISO, ma senti di avere ancora alcune lacune nelle tue conoscenze, troverai questo libro molto utile.

Questo libro fornisce esempi di gestione di politiche, procedure, piani e altri documenti in organizzazioni di piccole e medie dimensioni (cioè aziende con un massimo di 500 dipendenti). Tutti i principi qui descritti sono applicabili anche a organizzazioni più grandi, quindi potrai trovare utile questo libro anche se lavori per un'azienda più grande, tuttavia tieni presente che in alcuni casi le soluzioni dovranno essere più complesse di quelle descritte in questo libro.

Questo libro non è scritto come una guida per condurre gli audit, ma potrebbe essere utile per gli auditor interni o addirittura gli auditor di certificazione, per aiutarli a comprendere tutti i requisiti della norma e presentare inoltre la migliore pratica per scrivere la documentazione - questo sarà utile quando l'auditor dovrà scrivere delle raccomandazioni nel proprio rapporto di audit.

Penso che questo libro possa essere molto utile anche per i consulenti - come consulente, ho fatto uno sforzo per presentare in questo libro il modo più logico di gestire i documenti, per cui leggendolo attentamente potrai acquisire il know-how per i tuoi futuri Incarichi di consulenza.

Quindi, se sei un responsabile della produzione, un ingegnere, un responsabile della conformità, un professionista della sicurezza dell'informazione, un responsabile di un reparto di IT, un dirigente, un auditor interno, un consulente o un responsabile di progetto incaricato di implementare una norma ISO in una piccola o media impresa, questo libro è perfetto per te.

1.3 Come leggere questo libro

Ecco alcune delle caratteristiche di questo libro che ti renderanno più facile leggerlo e utilizzarlo nella pratica:

- Quando alcuni paragrafi di questo libro sono correlati a una clausola particolare delle norme ISO, questa clausola viene riportata nel titolo del paragrafo.
- Dal momento che il capitolo 3 descrive la documentazione relativa a determinate clausole della norma, la maggior parte dei paragrafi conterranno questi elementi:
    - Scopo – descrive brevemente il motivo dell'esistenza della clausola in oggetto e come questa possa essere utilizzata per il tuo sistema di gestione
    - Elementi in ingresso – quali input devi avere per implementare il requisito

  - Opzioni – quali opzioni vanno considerate nell'implementazione del requisito
  - Decisioni – quali decisioni devi prendere per proseguire
  - Documentazione – descrive come documentare i requisiti della norma ISO
  - Suggerimenti relativi alla documentazione – riepilogano brevemente i documenti necessari per ogni requisito

- Alcune sezioni contengono suggerimenti relativi a strumenti gratuiti che consentono di implementare la norma in modo più semplice.
- Alla fine dei capitoli 2 e 3 vedrai un paragrafo intitolato "Fattori di successo" che sottolineerà quello su cui ti dovrai concentrare.
- Alla fine del libro, nel capitolo 4, vedrai un breve caso studio che spiega come risolvere i problemi relativi alla documentazione in situazioni reali.
- Troverai molte informazioni utili negli allegati – il glossario, la checklist della documentazione obbligatoria per le principali norme ISO e la struttura della documentazione per l'Allegato A della ISO 27001

1.4 Quello che non troverai in questo libro

Questo libro è incentrato su come gestire la documentazione per le norme ISO, ma non spiega come implementare una norma – nella sezione 1.5 troverai il link per i corsi gratuiti online che spiegheranno tutto sull'implementazione.

Questo libro non ti fornirà dei modelli già compilati per tutte le tue politiche, procedure e piani, tuttavia ti spiegherà come preparare la tua azienda a scrivere i documenti di cui hai realmente bisogno e i documenti che ti saranno utili invece che costituire un ostacolo per la tua azienda. Tuttavia, non ti spiegherà come scrivere in dettaglio ogni singolo documento. Nell'Allegato A troverai un elenco dei documenti obbligatori per ognuna delle principali norme ISO, oltre a un elenco di documenti non obbligatori ma usati comunemente.

Questo libro non è una copia di una qualsiasi norma ISO - non puoi sostituire la lettura della norma con la lettura di questo libro. Questo libro intende spiegare come interpretare la norma (dal momento che la norma è scritta in maniera piuttosto ostica) e che tipo di conformità l'auditor si aspetta di trovare.

Quindi, per favore, non commettere l'errore di avviare l'implementazione e scrivere i documenti senza avere prima letto la norma - penso che troverai che questo libro insieme alla norma ISO siano la combinazione perfetta per il tuo futuro lavoro. Puoi acquistare la norma presso il sito ufficiale della ISO.

1.5 Ulteriori risorse

Ecco alcune risorse che ti aiuteranno, insieme a questo libro, a conoscere le varie norme ISO:

- Corsi ISO online – corsi gratuiti online che ti insegneranno le basi delle norme ISO 9001, ISO 14001 e ISO 27001, compresi alcuni suggerimenti su come creare la documentazione.
- Download gratuiti ISO 27001, download gratuiti ISO 9001 e download gratuiti ISO 14001 – una raccolta di libri bianchi, checklist, diagrammi, modelli ecc.

- Conformio – un sistema di gestione documentale (SGD) basato su cloud e uno strumento di gestione dei progetti incentrato sulle norme ISO.

- Kit Documentazione ISO 9001 – un set contenente tutti i modelli dei documenti richiesti dalla ISO 9001, che include l'assistenza da parte di un esperto che ti condurrà passo dopo passo verso la certificazione. Kit analoghi sono disponibili per altre norme ISO.

- La pagina ufficiale del sito web della ISO, Official ISO webpage – qui potrai acquistare la versione ufficiale di tutte le norme ISO.

2
PREPARARSI A SCRIVERE I DOCUMENTI

Uno dei motivi più comuni per il fallimento dei progetti di implementazione delle norme ISO è che le aziende si sono precipitate ad avviare tali progetti senza una corretta preparazione. E parte di quella preparazione consiste nel decidere cosa fare con la documentazione.

Quindi, ecco a cosa devi pensare prima di avviare il progetto:

2.1 Tre opzioni per l'implementazione della norma e la scrittura della documentazione

All'inizio dell'implementazione ISO, sarai probabilmente sopraffatto dai vari approcci su come avviare e completare con successo questo progetto. A mio avviso, esistono tre opzioni fondamentali per implementare queste norme e scrivere tutti i documenti necessari: (1) farlo utilizzando soltanto i propri dipendenti, (2) utilizzare un consulente oppure (3) (a metà strada tra le altre due opzioni) implementare la norma con un approccio Fai-da-Te, sfruttando al contempo il know-how esterno.

Ma non tutti questi approcci sono applicabili a chiunque - ecco una spiegazione di ciascuna di queste opzioni e delle situazioni in cui si dimostrano appropriate.

1) Implementare la norma utilizzando i tuoi dipendenti. Ossia quando decidi di implementare la norma senza alcun aiuto

esterno, usando solo la conoscenza e la capacità dei tuoi dipendenti. Questa opzione implica che i tuoi dipendenti eseguano tutte le analisi, facciano tutte le interviste, scrivano la documentazione, ecc.

Pro. Questa è probabilmente l'opzione più economica perché non dovrai pagare per avere un servizio esterno. Inoltre non consentirai a nessun professionista esterno alla tua azienda di scoprire qualcosa sui processi o la documentazione interni. Infine, scrivere la propria documentazione accrescerà l'impegno dei tuoi dipendenti nei confronti dei cambiamenti richiesti.

Contro. Questa è probabilmente l'opzione che richiederà più tempo perché starai facendo tutto da solo. Inoltre, se i tuoi dipendenti non sono esperti o abbastanza competenti, potrebbe rivelarsi l'opzione più costosa a causa degli errori che questi potrebbero fare.

2) Usare un consulente. Questa opzione implica l'assunzione di un esperto esterno (di solito un consulente locale) che abbia esperienza nell'implementazione della norma - questa persona eseguirà l'analisi della tua azienda, farà le interviste, scriverà la documentazione e tutto il resto - fondamentalmente implementerà l'intera norma per tuo conto.

Pro. Questo è sicuramente il modo più veloce per implementare la norma - se assumi un buon consulente, questi avrà molta esperienza e saprà organizzare il progetto per completarlo rapidamente. È anche la soluzione migliore se i tuoi dipendenti non hanno il tempo di dedicarsi a questo progetto. Inoltre, quando le cose devono cambiare, la direzione potrebbe avere più fiducia in qualcuno esterno all'azienda.

Contro. I consulenti ovviamente costano denaro, quindi questa è l'opzione più costosa. Inoltre, in questo modo fornirai a una persona esterna l'accesso a quasi tutti i segreti aziendali (ad

esempio, come è organizzata l'azienda, i suoi processi principali e i vantaggi competitivi chiave, chi sono le persone più importanti, ecc.). Inoltre, se qualcuno dall'esterno scrive la documentazione, i dipendenti potrebbero avere la sensazione che le politiche e le procedure gli vengano imposte, così spesso potrebbero cercare di aggirarle. Infine, una volta che il consulente se ne va, molto spesso i dipendenti non riescono a mantenere la documentazione perché non hanno acquisito tutte le conoscenze necessarie.

3) Implementare la norma con un approccio Fai da Te e usando il know how esterno. Questa opzione è diventata molto popolare negli ultimi due anni ed è fondamentalmente qualcosa che si trova a metà tra le prime due opzioni. Con questo metodo, i tuoi dipendenti effettueranno tutta l'implementazione, ma avendo a disposizione il know-how, la documentazione e il supporto di una parte esterna.

Pro. Questa opzione non è costosa come lo sono i consulenti, e ti fornirà comunque tutto il know-how e il supporto necessari. Inoltre, non darai accesso alle informazioni riservate a qualcuno esterno all'azienda. Infine, poiché saranno i tuoi dipendenti a scrivere la documentazione, il loro impegno a seguire le nuove regole sarà probabilmente maggiore.

Contro. I dipendenti dovranno imparare come effettuare l'implementazione, quindi non è il modo più rapido per implementare la norma. Inoltre, questa opzione non risolve il problema se i tuoi dipendenti sono completamente assorbiti da altri progetti e non hanno assolutamente tempo per nuovi incarichi.

Quindi, quale opzione scegliere? Dovresti implementare la norma utilizzando i tuoi dipendenti, se hai dei dipendenti già esperti nell'implementazione, se hai dei dati molto riservati e se il tuo budget è molto basso. D'altra parte, se hai fretta e non

temi che alcuni segreti aziendali possano essere esposti, allora dovresti usare un consulente. Ovviamente, per questa opzione dovrai avere a disposizione un buon budget. Infine, scegli l'opzione dell'implementazione Fai da Te se desideri che i tuoi dipendenti imparino come fare questo lavoro, se non hai troppa fretta, se il tuo responsabile di progetto può dedicarci un paio d'ore al giorno, e, naturalmente, se il tuo budget non è troppo elevato.

2.2 La sequenza della scrittura della documentazione e il rapporto con il ciclo PDCA

La buona notizia è che le norme ISO hanno reso più facile implementarle e scrivere la documentazione mostrando le fasi per l'implementazione in ordine successivo.

Tutte le norme conformi all'allegato SL (ad es. ISO 9001, ISO 14001, ISO 27001, ISO 22301) sono scritte in modo chiaro e sequenziale, per cui fondamentalmente le fasi dell'implementazione dovrebbero seguire quasi esattamente la stessa sequenza della norma scritta. O, per essere più precisi, le fasi del tuo piano di progetto dovrebbero assomigliare alle clausole dalla 4 alla 10 di tali norme, nell'ordine in cui sono scritte.

Naturalmente, gli elementi in uscita della maggior parte delle fasi dell'implementazione saranno vari documenti: sarà necessario produrre tutti i documenti obbligatori, oltre a tutti i documenti che deciderai essere necessari per la tua azienda. Troverai gli elenchi dei documenti obbligatori negli allegati di questo libro e nella sezione 3.4 ti spiegherò come decidere quali documenti non obbligatori scrivere.

Questa sequenzialità è una conseguenza della norma che viene scritta seguendo il cosiddetto ciclo Plan-Do-Check-Act (PDCA),

secondo il quale, per avere un sistema di gestione efficace, devi prima pianificare ciò che intendi fare (compresa la definizione degli obiettivi), quindi dovrai implementare (la fase Do) quello che hai pianificato, poi controllare (Check) se l'implementazione ha raggiunto i risultati attesi e, infine, dovrai colmare il divario (fase Act) tra quello che hai raggiunto e quello che avevi inizialmente pianificato. Poiché le clausole dalla 4 alla 10 seguono esattamente questa logica, anche tu dovrai seguirla.

Si prega di notare che quando in questo libro uso la parola *implementazione* non significa necessariamente solo la fase di implementazione (Do) nel ciclo PDCA - con *Implementazione* intendo le fasi necessarie per applicare tutti i requisiti di una norma specifica, indipendentemente dalla fase del ciclo PDCA a cui appartengono.

Suggerimento per uno strumento gratuito: Conformio è uno strumento online che copre tutte le fasi dell'implementazione di ISO 9001, ISO 14001 e ISO 27001 e contiene le linee guida per ognuna delle fasi dell'implementazione.

2.3 Usare strumenti e modelli

Quando inizi l'implementazione di una struttura complessa come una norma ISO, probabilmente cercherai un modo per rendere il tuo lavoro più facile. Chi non lo farebbe? Dopo tutto, inventare di nuovo la ruota non è un lavoro molto interessante.

Ma stai attento quando inizi a cercare questi strumenti - non tutti gli strumenti ti aiuteranno: potresti finire con una ruota di camion che non si adatta alla macchina che stai guidando.

(Questa parte del libro non viene mostrata nell'anteprima gratuita)

BIBLIOGRAFIA

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

INDICE

Gestire la Documentazione ISO: Una Guida in Linguaggio Semplice

Una Guida Passo dopo Passo per Professionisti ISO in Aziende di Piccole Dimensioni

Pensa e agisci come un consulente con questa guida pratica per la gestione della documentazione ISO.

L'autore ed esperto consulente ISO Dejan Kosutic condivide la propria conoscenza e il suo senso pratico in un libro dal valore inestimabile. Apprenderai:

- ✓ La sequenza di scrittura della documentazione
- ✓ Come decidere sulla strategia della documentazione
- ✓ Se utilizzare strumenti e modelli
- ✓ Come controllare i documenti e le registrazioni
- ✓ Quali sono i documenti obbligatori
- ✓ Come decidere quali documenti non obbligatori scrivere
- ✓ Come scrivere dei documenti che siano accettati dai tuoi colleghi
- ✓ Tutto questo e molto altro ancora ...

Scritto in linguaggio di facile comprensione, *Gestire la Documentazione ISO: Una Guida in Linguaggio Semplice* è scritto per le persone che gestiscono i documenti ISO per la prima volta e hanno bisogno di indicazioni chiare su come farlo. Che tu sia un professionista esperto o nuovo nel settore, questo è l'unico libro sull'argomento di cui avrai bisogno.