PREPARARSI ALL'AUDIT DI CERTIFICAZIONE ISO: UNA GUIDA IN LINGUAGGIO SEMPLICE

ISO

03

COLLANA LIBRI TASCABILI

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

DEJAN KOSUTIC

Prepararsi all'Audit di Certificazione 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

Dejan Kosutic

Prepararsi all'Audit di Certificazione 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: 978-953-8155-13-0

Prima Edizione, 2017

Titolo originale: "Preparing for ISO Certification Audit: 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 informatica 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 all'inizio di quest'anno 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 preparare la propria azienda per la certificazione ISO.

È per questo motivo che ho creato questo libro più breve, parte della collana di manuali, incentrato esclusivamente sul processo di certificazione e su come prepararsi ad affrontare questo processo. Questo libro non riguarda esclusivamente la ISO 27001 - il processo di certificazione è lo stesso 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, *Prepararsi all'Audit di Certificazione ISO: Una Guida in Linguaggio Semplice*, è in realtà un estratto dal libro *Sicuro & Semplice* che ho modificato eliminando soltanto qualche dettaglio. Se lo confronti con le sezioni di *Sicuro & Semplice* che parlano di certificazione, 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 preparazione della certificazione e non hanno il tempo (o la necessità) di leggere un libro dettagliato sull'implementazione delle norme ISO, ossia un libro come *Sicuro & Semplice*.

Potresti anche essere sconcertato dal fatto che questo libro sia piuttosto breve, mentre esistono sul mercato altre opere molto più lunghe e dettagliate sulla certificazione ISO. 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 preparazione alla certificazione nelle aziende più piccole, pertanto ho intenzionalmente semplificato i passaggi, in modo che la tua preparazione si possa svolgere piuttosto rapidamente, 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 prepararti per l'audit di certificazione. E vedrai i reali vantaggi dell'ottenere la certificazione per la tua azienda.

1
INTRODUZIONE

Per quale motivo la tua azienda dovrebbe decidere di ottenere una certificazione ISO? Come si differenzia la certificazione aziendale dalla certificazione personale? E ancora, questo libro è quello che ti serve?

Questo libro tratta del processo di certificazione 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 mi riferisco a una "norma ISO" o semplicemente a una "norma", intendo qualunque norma tra quelle sopra elencate.

1.1 Perché la tua azienda dovrebbe scegliere di ottenere una certificazione?

Prima di decidere se la tua azienda debba intraprendere il percorso per ottenere la certificazione, devi porti una domanda importante: ne hai veramente bisogno?

Devo dirti che ci sono molte organizzazioni che hanno implementato la norma scegliendo di non certificarsi - un esempio evidente sono le banche e altri istituti finanziari. I regolamenti nella maggior parte dei paesi sono tali che questi istituti sono obbligati a implementare procedure e garanzie di sicurezza dell'informazione molto rigide, e la maggioranza di essi lo fa utilizzando la norma ISO 27001. Tuttavia, pochissimi tra questi sono certificati: hanno concluso che non c'era alcun motivo aziendale per farlo.

Questo è esattamente ciò che devi fare: valutare attentamente se hai bisogno del certificato. Ecco i potenziali motivi per cui potresti trovare utile la certificazione:

1) Marketing. Puoi utilizzare il certificato per acquisire nuovi clienti (ad esempio, partecipando a gare d'appalto) o per rimanere in attività (ad esempio, se tutti i tuoi concorrenti hanno già il certificato).

2) Conformità. Raramente, alcuni regolamenti richiedono l'implementazione di particolari norme ISO, ma potrebbe anche verificarsi dei casi, per esempio, in cui firmi dei contratti con clienti che ti impongono di implementare un Sistema di gestione della qualità conforme alla

3) ISO 9001. Invece di doverti sottoporre alle verifiche degli auditor di ciascuno dei tuoi clienti che vogliono controllare se hai adempiuto al contratto, puoi fare in modo che sia l'auditor di certificazione a fare questo lavoro, e poi mostrare il certificato a tutti i tuoi clienti.

4) Pressione interna. In alcune aziende, questi tipi di progetti non arriveranno mai a conclusione a meno che non ci sia una forte pressione - come una scadenza definita. Quindi, se fissi con l'ente di certificazione una data per l'audit di certificazione, sia la tua direzione che i tuoi dipendenti avranno un senso di urgenza molto più forte per completare il progetto.

5) Input obiettivi. Se vuoi che la tua sicurezza delle informazioni venga implementata nel migliore dei modi, è bene chiamare delle persone con una vasta esperienza e che sappiano in che modo tu possa confrontarti con i migliori del settore. Gli auditor di certificazione saranno più che felici di verificare qualcuno che ce la sta

mettendo tutta e ti forniranno degli input su ciò che potresti migliorare.

Se pensi che almeno uno di questi vantaggi sia applicabile alla tua azienda, probabilmente dovresti decidere di ottenere la certificazione. Ma è vero anche il contrario: se non ti rifletti in nessuno dei punti elencati, probabilmente la tua azienda non ha affatto bisogno del certificato.

1.2 Certificazione, registrazione e accreditamento a confronto

Prima di approfondire l'argomento della certificazione, cerchiamo di chiarire innanzitutto alcune questioni di base.

Come funziona la certificazione aziendale. Innanzitutto, le norme ISO sono pubblicate dall'International Organization for Standardization - un organismo internazionale fondato dai governi di tutto il mondo. Il suo scopo è quello di pubblicare le norme come un modo per diffondere la conoscenza e le migliori pratiche - finora, sono state pubblicate in totale quasi 20.000 norme, riconosciute in ogni paese.

Le norme di gestione ISO, create principalmente come un aiuto alle aziende per migliorare le proprie attività in determinate aree (ad esempio, la ISO 9001 per la gestione della qualità, la ISO 27001 per la gestione della sicurezza delle informazioni, ecc.), sono solo una parte di queste 20.000 norme. È per questa ragione che la maggior parte delle discussioni su queste norme è legata alle imprese e alla loro registrazione, certificazione e accreditamento.

Certificazione vs. registrazione. Quando si vuole dire che un'azienda ha implementato una norma (ad esempio, un sistema di gestione ambientale conforme alla ISO 14001), ha

completato con successo l'audit di certificazione e l'ente di certificazione ha emesso il certificato, la si chiama registrazione o certificazione.

Nel Nord America, è comunemente usato il termine "registrazione", mentre nel resto del mondo di solito si dice "certificazione". Ma c'è una differenza? Tecnicamente, sì, ma in sostanza, no.

La certificazione è quando un ente di certificazione emette il certificato che dimostra che un'azienda è conforme a una norma. La registrazione avviene quando questo certificato è registrato presso l'ente di certificazione. Quindi, fondamentalmente, si tratta della stessa cosa: un'azienda ha ottenuto un certificato che è formalmente riconosciuto.

Comunque, l'International Organization for Standardization raccomanda l'uso del termine "certificazione", per cui d'ora in avanti userò questo termine.

Ente di certificazione vs. registrar. Questa è una differenza di terminologia che deriva direttamente dall'uso dei termini certificazione / registrazione - nel Nord America le persone di solito usano il termine registrar, mentre nel resto del mondo sono chiamati enti di certificazione.

Ma anche in questo caso si tratta della stessa cosa: sono gli istituti che eseguono gli audit di certificazione e che emettono i certificati. Anche qui, l'ISO consiglia di utilizzare il termine "ente di certificazione".

Accreditamento vs certificazione. Cos'è allora l'accreditamento? Perché gli enti di certificazione possano condurre gli audit di certificazione ed emettere i certificati, devono ottenere una licenza, e questa licenza è chiamata "accreditamento". Quindi, gli enti di certificazione vengono accreditati, mentre le aziende vengono certificate. (L'ente di certificazione deve essere

conforme alla norma ISO 17021 se desidera ottenere l'accreditamento per la certificazione dei sistemi di gestione.)

Di solito c'è un solo ente di accreditamento per ogni paese (ad esempio, UKAS per il Regno Unito), mentre esistono diversi enti di certificazione operanti in ciascun paese, che vanno dai piccoli enti di certificazione locali alle grandi multinazionali come SGS, BSI, DNV, Bureau Veritas, eccetera.

La cosa buona degli enti di accreditamento è che di solito pubblicano l'elenco degli enti di certificazione accreditati nei loro paesi - vedi l'elenco degli enti di certificazione nel Regno Unito e l'elenco degli enti di certificazione negli Stati Uniti.

Tuttavia, anche gli enti di accreditamento devono essere conformi a una norma, la ISO 17011, una norma che definisce il processo di accreditamento.

La certificazione delle persone. Tutto quanto menzionato sopra è valido per la certificazione delle aziende - se desideri ottenere una certificazione personale, le cose sono un po' diverse. Sono stati sviluppati molti corsi sulle norme ISO al fine di aiutarti a implementare o verificare una norma in un'azienda. Questo è anche il motivo per cui esistono delle certificazioni e degli accreditamenti relativi a tale settore formativo.

Per quanto riguarda l'accreditamento, esiste un modello simile a quello descritto sopra - se un istituto vuole fornire certificati di formazione, deve essere accreditato da un ente di accreditamento e in questo caso tale istituto deve essere conforme alla norma ISO 17024.

Ecco alcuni degli istituti di formazione accreditati più popolari: PECB, IRCA, Exemplar Global (ex RABQSA), ecc.

La certificazione personale a confronto con la certificazione della formazione. Nella maggior parte dei casi, gli istituti di

formazione accreditati non offrono i corsi direttamente agli studenti: piuttosto hanno una rete di partner - fornitori di formazione - che erogano i corsi sotto la loro licenza e supervisione.

Questo rapporto tra istituti accreditati e fornitori di formazione di solito opera in due modi: a) i fornitori di formazione utilizzano i corsi sviluppati dagli istituti accreditati, dopo di che è l'istituto accreditato a rilasciare i certificati direttamente agli studenti; oppure b) l'organizzazione di formazione sviluppa i propri corsi e un istituto accreditato certifica tali corsi - in questo caso, è comune che sia l'organizzazione che eroga la formazione a rilasciare il certificato agli studenti, con l'approvazione dell'istituto accreditato.

Ci sono numerose organizzazioni di formazione in tutto il mondo - che vanno dagli enti di certificazione che offrono anche la certificazione delle organizzazioni, ai piccoli istituti specializzati e fornitori di corsi online.

Vale la pena ricordare che la certificazione dei corsi è obbligatoria per i fornitori di formazione che erogano corsi come quello per Lead Auditor, perché questo è l'unico modo per ottenere il riconoscimento da parte degli enti di certificazione che assumeranno gli auditor con tali certificati. Tuttavia, per altri corsi più brevi, i fornitori di formazione spesso scelgono di non certificare i propri corsi perché non ritengono importante tale riconoscimento e considerano il loro marchio sufficiente a garantire la qualità del corso.

1.3 Chi dovrebbe leggere questo libro?

Questo libro è scritto soprattutto per i principianti nel settore e per le persone con una conoscenza non approfondita sulla certificazione ISO - ho strutturato questo libro in modo tale che

una persona che non abbia esperienze o conoscenze precedenti sulle norme ISO possa comprendere rapidamente il funzionamento di tutto il processo di certificazione e quali siano le fasi per il suo positivo completamento. D'altra parte, anche se hai già esperienza di certificazioni ISO ma senti di avere ancora alcune lacune su questo argomento, troverai questo libro molto utile.

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

Penso che questo libro possa essere molto utile anche ai consulenti, - essendo anch'io un consulente, ho fatto uno sforzo per presentare in questo libro il modo più logico di prepararsi all'audit di certificazione, quindi leggendo attentamente questo libro potrai acquisire il know- how per i tuoi futuri incarichi di consulenza.

1.4 Quello che non troverai in questo libro

Questo libro riguarda la certificazione delle aziende, non parla di come certificare le persone. Anche se sia le aziende che le persone possono ottenere un certificato ISO, lo scopo e il processo delle relative certificazioni sono molto diversi.

Questo libro è focalizzato sulle fasi del processo di certificazione e su come prepararsi per la certificazione, ma non spiega come implementare la norma - nella sezione 2.1 troverai dei link ad alcuni articoli che spiegano le fasi dell'implementazione.

Questo libro non ti fornirà dei modelli già compilati per tutte le tue politiche, procedure e piani, tuttavia ti spiegherà quali sono i documenti che l'auditor di certificazione vorrà verificare.

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 la certificazione a fronte di una norma senza averla letta prima - 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.
- 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 27001 – un set di tutti i modelli dei documenti richiesti dalla ISO 27001, che includono

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
ASSICURARSI CHE L'AZIENDA SUPERI L'AUDIT DI CERTIFICAZIONE

Francamente, non ho mai conosciuto nessuno che si sia goduto la certificazione. Nella maggior parte dei casi, tutti la considerano un male necessario e odiano il giorno in cui finalmente arriva l'auditor (o quel giorno si danno malati).

Ma non è necessario che sia così – puoi ottenere qualcosa da tutto questo, oltre, ovviamente, al certificato. Come spiegherò in seguito, gli auditor di certificazione sono persone esperte con una perfetta visione delle pratiche migliori e si può imparare molto da loro. Ma bisogna approcciarli nel modo giusto.

2.1 Le fasi precedenti alla certificazione – il controllo finale

Naturalmente, prima di arrivare alla certificazione, bisogna applicare la norma. Poiché questo libro non ha l'obiettivo di descrivere l'implementazione, di seguito ci sono i link ad alcuni articoli che ti aiuteranno nell'implementazione:

- Checklist of ISO 9001 implementation & certification steps
- Elenco delle fasi dell'implementazione della ISO 14001
- ISO 27001 implementation checklist

- 17 steps for implementing ISO 22301
- 12 steps for ISO 20000 implementation
- 12 Steps for implementation and certification against OHSAS 18001

Bene, hai lavorato all'implementazione della ISO per mesi e mesi, hai cercato di capire come renderla più facile leggendo libri e articoli, hai convinto non solo i tuoi colleghi ma anche la direzione che questa norma è molto utile, ma hai ancora un problema: hai dei preconcetti.

Questo progetto è il tuo bambino e potresti essere incline a credere che i documenti e tutto ciò che hai preparato siano impeccabili. Ma non è mai così – c'è sempre qualcosa che viene tralasciata, puoi avere persino interpretato qualche requisito nel modo sbagliato, forse hai dimenticato qualcosa. Oppure il problema non sei tu – forse c'è qualcun altro responsabile, ad esempio, della misurazione, che non fa correttamente il proprio lavoro.

Tutto questo significa che potresti avere dei problemi durante l'audit di certificazione. Per evitare tutto ciò, ti consiglio di fare un controllo finale, che possa darti un quadro chiaro di cosa sia necessario correggere prima della certificazione.

Fondamentalmente, il trucco è questo:

- In primo luogo, controllare se **l'audit interno, il riesame della direzione** e **le azioni correttive** sono stati eseguiti.
- Quindi, controllare l'elenco dei documenti obbligatori e vedere se ci sono tutti. Questi articoli ti potranno aiutare:
    - Elenco dei documenti obbligatori richiesti dalla ISO 9001:2015

- Elenco dei documenti obbligatori richiesti dalla ISO 14001:2015
- List of mandatory documents required by ISO 27001 (2013 revision)
- Mandatory documents required by ISO 22301
- List of mandatory documents required by OHSAS 18001

- Controlla che siano stati implementati tutti i **processi e i controlli che hai pianificato di implementare** - ad esempio, nella ISO 27001 i controlli sono pianificati tramite il documento denominato Piano del trattamento dei rischi.

- Quindi, leggi di nuovo la norma e verifica che la **documentazione sia conforme a tutti i requisiti** che la norma prevede.

- Infine, e questa è la parte più difficile: **dovrai girare per tutta l'azienda** (dovrai anche visitare alcuni dei tuoi partner / fornitori che hanno un ruolo nel tuo sistema) comportandoti come se fossi l'auditor di certificazione. Questo significa che dovrai chiedere a tutte le persone una sola domanda molto semplice: Fai tutto ciò che è scritto nella tua documentazione? Devi solo leggere quello che è scritto in tutti i tuoi documenti (politiche, procedure, piani, ecc.) e verificare se le risposte ricevute sono adeguate. Per scoprire la verità, non bisogna fare affidamento solo sulle loro risposte - bisogna scavare più in profondità e cercare le registrazioni che dimostrino quello che le persone intervistate stanno dicendo.

Questo è tutto: una volta svolti questi compiti per ciascuna delle tue attività, per ognuno dei tuoi documenti, per ognuno dei tuoi

principali fornitori e partner, avrai un bel quadro di ciò che funziona e di cosa debba invece essere risolto.

Se guardi più da vicino, ti accorgerai che queste attività assomigliano molto a quelle che vengono svolte da un auditor interno. Allora, perché farlo? Innanzitutto, gli auditor interni sono di solito persone inesperte e non ci si può aspettare molto dalla prima volta che fanno questo lavoro; in secondo luogo, sei tu il responsabile del successo del progetto e probabilmente vorrai assicurarti che tutto sia pronto.

Puoi anche assumere un professionista esterno per eseguire questo controllo finale - può essere fatto dal tuo consulente se ne hai uno - è vero che non può condurre un audit interno a causa del conflitto di interessi, ma niente ti impedisce di assumerlo per questo controllo finale. E se il consulente ha esperienza nello svolgimento degli audit, tanto meglio.

Vedi anche il mini caso studio del capitolo 3: Mini caso studio: Preparare una società di telecomunicazioni alla certificazione.

2.2 Come scegliere un ente di certificazione

Il prezzo è, ovviamente, il criterio principale per scegliere il tuo ente di certificazione e, naturalmente, dovrai chiedere dei preventivi a un paio di enti di certificazione, per vedere cosa sia incluso nel prezzo.

Tuttavia, il prezzo non è tutto - ecco alcune altre cose da considerare quando si sceglie con chi lavorare:

- Reputazione. Se vuoi utilizzare il certificato per finalità di marketing, probabilmente non vorrai ottenere il certificato da un organismo che è noto per distribuirli senza alcun criterio. Dovrai scegliere un ente di

certificazione con una reputazione solida, se non perfetta.

- L'accreditamento. In realtà, chiunque può dare un pezzo di carta dicendo che sei certificato ISO ma, purtroppo, non tutti gli enti di certificazione sono accreditati per farlo – pertanto, è necessario accertarsi che l'ente di certificazione abbia un accreditamento.

- Specializzazione. Se sei una banca, non è esattamente una buona idea avere un ente di certificazione che finora ha certificato solo imprese manifatturiere. Se l'auditor finora ha verificato solo imprese manifatturiere, perderai troppo tempo per spiegargli come funziona una banca - di conseguenza, avrà imparato molto di più lui da te che non tu da lui.

- Esperienza. Anche se potresti desiderare qualcuno con scarsa esperienza per superare facilmente l'audit, è effettivamente nel tuo interesse avere un auditor esperto (vedere la sezione 2.5). Quindi, non avere paura di chiedere quale auditor ti verificherà e di richiedere il suo CV e / o un elenco delle società che ha verificato.

- Audit integrato. Potresti iniziare solo con la ISO 9001, ma se prevedi di implementare anche la ISO 14001, la ISO 27001 e altre norme, puoi chiedere all'ente di certificazione di effettuare un cosiddetto audit integrato. Questo significa che non dovrai superare audit separati per ciascun sistema (e pagare la quota intera per ciascuno di essi), ma un solo audit per tutti questi sistemi. In questo modo, non solo risparmierai tempo (l'audit di un sistema integrato ha una durata inferiore di quella totale dei diversi audit condotti separatamente), ma ti costerà anche di meno.

- Flessibilità. Se l'ente di certificazione deve far venire l'auditor in aereo da un altro continente (perché non ha nessuno a livello locale), in caso di imprevisti dell'ultimo momento (ad esempio, se non hai completato il progetto o si è verificato qualche problema) sarà molto difficile cambiare la data dell'audit, dato il viaggio sarà già completamente organizzato.

- Lingua. Anche se l'ente di certificazione fosse in grado di fornire un traduttore in caso l'auditor (o gli auditor) non parlasse la tua lingua, un audit condotto da un auditor con il quale non esistano barriere linguistiche si svolgerebbe sicuramente in modo più facile: l'auditor sarebbe in grado di leggere molto più agevolmente i tuoi documenti e, non avendo difficoltà di comunicazione, ti sarebbe possibile sviluppare un migliore rapporto con lui.

Quindi, si tratta di questo - come con qualsiasi altro fornitore, dovrai fare i tuoi compiti e scegliere cosa è meglio per te. E, ricorda: devi considerare sia il costo totale del servizio che stai ricevendo che il costo dell'opportunità persa - un ente di certificazione a basso costo potrebbe richiedere troppo tempo e dare poco valore in cambio.

Vedi anche Allegato A per un elenco dettagliato delle domande che dovresti rivolgere ai potenziali enti di certificazione.

2.3 Le fasi della certificazione aziendale e come prepararsi

Nel processo di certificazione ci sono fondamentalmente tre fasi:

1) Lo stage 1 di Audit - chiamato anche Riesame della documentazione,

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

BIBLIOGRAFIA

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

INDICE

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

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

Pensa e agisci come un professionista esperto con questa esauriente e pratica guida passo dopo passo per la certificazione a fronte delle norme ISO 9001, ISO 14001, ISO 27001, o qualsiasi altra norma di gestione ISO.

Auditor e consulente esperto, Dejan Kosutic condivide la propria conoscenza e il suo senso pratico in un libro dal valore inestimabile. Apprenderai:

- ✓ I benefici della certificazione ISO per la tua azienda
- ✓ Tutte le fasi del processo di certificazione ISO
- ✓ Come scegliere l'ente di certificazione
- ✓ Quello che gli auditor di certificazione possono o non possono fare
- ✓ Come gestire le non conformità
- ✓ Come approcciarsi all'auditor di certificazione
- ✓ Tutto questo e molto altro ancora ...

Scritta in un linguaggio di facile comprensione, l'opera *Prepararsi all'Audit di Certificazione ISO: Una Guida in Linguaggio Semplice* è rivolta alle persone che stanno affrontando la certificazione ISO per la prima volta e che hanno bisogno di chiare indicazioni su come farlo. Che tu sia un professionista esperto o un principiante, questo è l'unico libro sull'argomento di cui avrai bisogno.