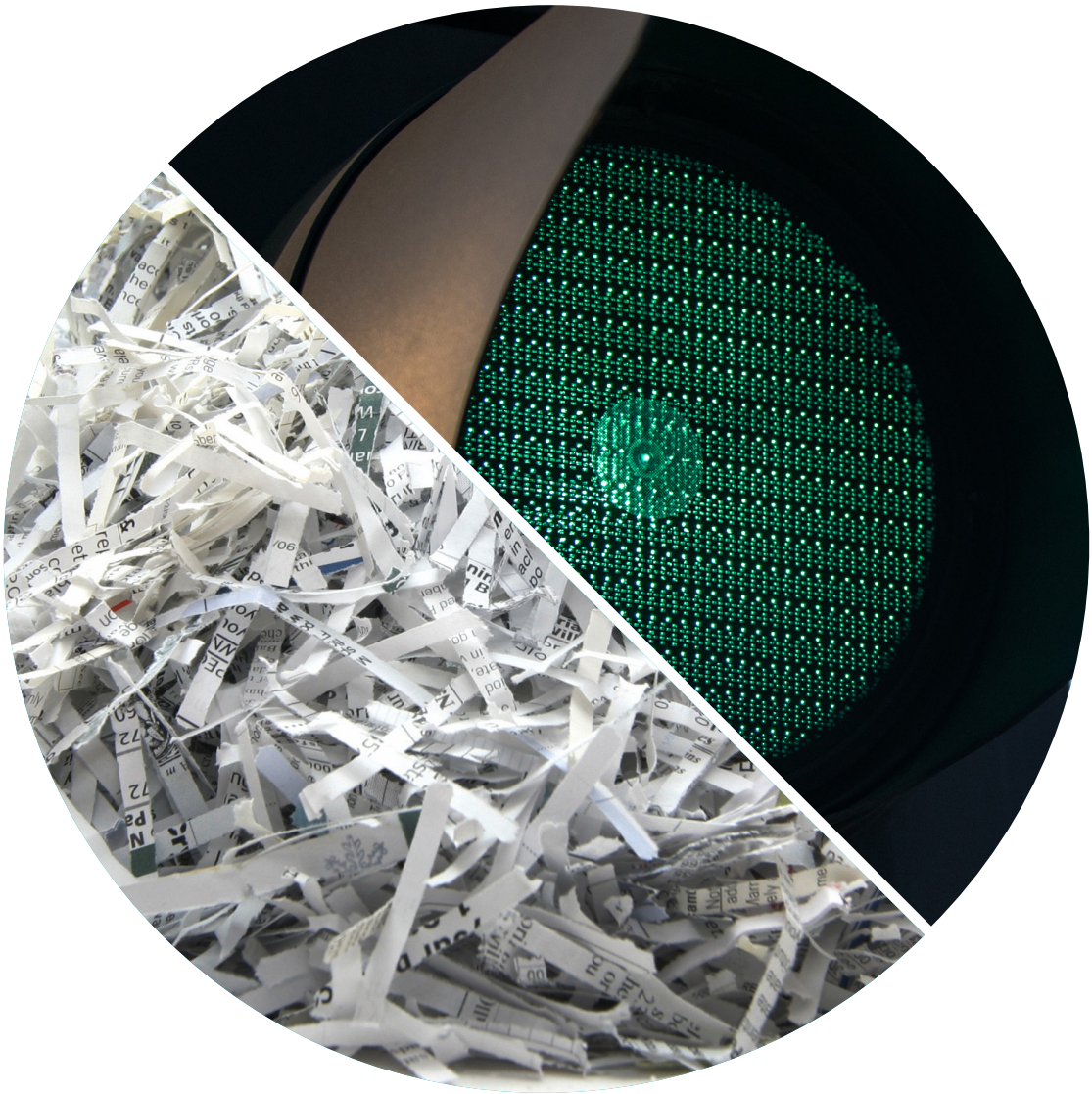
ISO/IEC 27001:2013

Guida all'implementazione



bsi.

...making excellence a habit.™

Cos'è lo standard **ISO/IEC 27001**?

Le aziende di successo conoscono il valore di informazioni tempestive e accurate, comunicazioni adeguate e riservatezza. La sicurezza delle informazioni riguarda sia lo sfruttamento delle opportunità del mondo interconnesso in cui viviamo sia la gestione del rischio.

Ecco perché le organizzazioni devono costruire un sistema resiliente attorno alla gestione della sicurezza delle informazioni. Riconosciuto a livello internazionale, lo standard **ISO/IEC 27001** è un framework eccellente che aiuta le organizzazioni a gestire e proteggere il patrimonio informativo in modo che sia protetto e sicuro.

In BSI disponiamo di esperienza, competenze e servizi di supporto per aiutarti a ottenere il massimo dallo standard **ISO/IEC 27001**, migliorando la resilienza e la capacità di risposta in caso di minacce al sistema informativo.

Questa guida illustra come implementare lo standard **ISO/IEC 27001** all'interno della tua organizzazione per consolidare la resilienza a lungo termine e salvaguardare la reputazione. Presentiamo inoltre i nostri servizi di supporto supplementari, per affiancarti non solo nel conseguimento della certificazione, ma anche per ridurre i rischi e proteggere l'attività.

"Lo standard ISO/IEC 27001 dimostra ai clienti che i nostri dati sono al sicuro e i sistemi sono robusti."

Hugo Holland Bosworth,
Direttore operazioni del gruppo,
Alternative Networks Plc

Contenuti

Come funziona lo standard **ISO 27001** e quali risultati assicura

La capacità di gestire le informazioni in maniera sicura e protetta non è mai stata così importante come ora. Lo standard ISO/IEC 27001, non solo ti aiuta a proteggere la tua 'attività, ma invia anche un chiaro segnale ai clienti, ai fornitori e al mercato che l'organizzazione è in grado di gestire le informazioni in modo sicuro.

ISO/IEC 27001 è un framework robusto che aiuta a proteggere informazioni come i dati finanziari, la proprietà intellettuale o le informazioni sensibili dei clienti. Consente di identificare i rischi e implementa misure di sicurezza adeguate, in modo che l'azienda possa gestire o ridurre i rischi per le informazioni. Consente di rivedere e perfezionare continuamente il modo in cui viene fatto, non solo per il presente, ma anche per il futuro. Ecco come lo standard ISO/IEC 27001 protegge il business e la reputazione e aggiunge valore.

Benefici dello standard ISO/IEC 27001:2013*

75% riduce il rischio aziendale

80% ispira fiducia nella nostra attività

71% aiuta a proteggere la nostra attività

55% ci aiuta a rispettare le normative

53% aumenta il nostro vantaggio competitivo

50% riduce la probabilità di errore

"Ha aiutato il team a comprendere le minacce e le vulnerabilità dell'ambiente attuale e a controllarle in maniera proattiva. Ha portato a una maggiore consapevolezza e attenzione alla sicurezza delle informazioni."

Mr. Tareq Al-Sahaf, Direttore generale. Gulf Insurance Group K.S.C (GIG)

*Fonte: BSI Benefits survey - BSI clients were asked which benefits they obtained from ISO/IEC 27001:2013

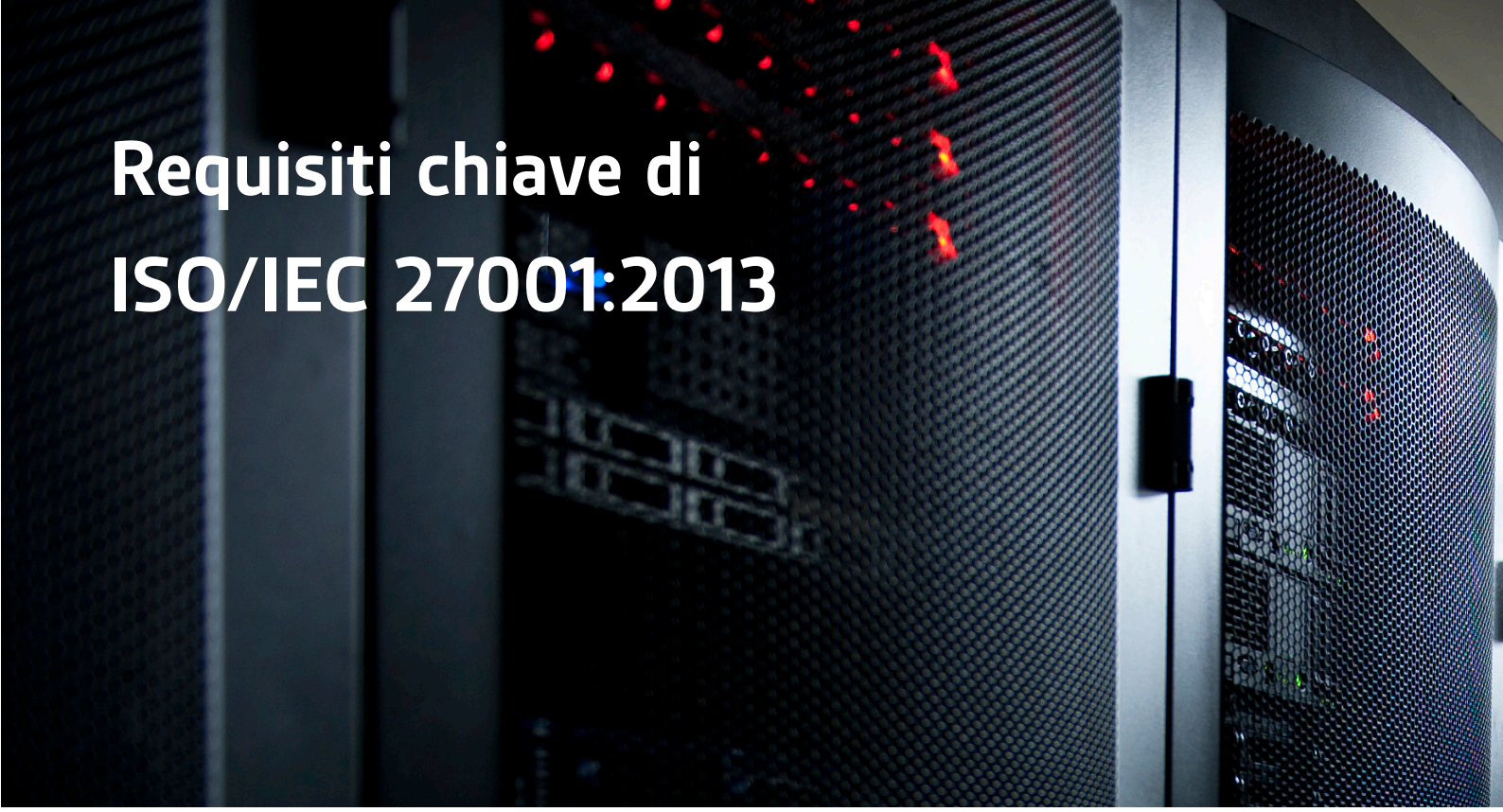
Come funziona lo standard **ISO/IEC 27001**

L'ultima versione dello standard **ISO/IEC 27001** è stata pubblicata nel 2013 per mantenerlo al passo con le sfide delle moderne attività e assicurarne l'allineamento con i principi della gestione del rischio contenuti nello standard ISO 31000. Si basa su una struttura di alto livello (Allegato SL), un framework comune per tutti gli standard del sistema di gestione ISO rivisti e futuri, inclusi gli standard ISO 9001:2015 e ISO 14001:2015.

L'Allegato SL aiuta ad assicurare coerenza, allineare i diversi standard del sistema di gestione, offrire clausole secondarie rispetto alla struttura di alto livello e applicare un linguaggio comune. Impone alle organizzazioni di incorporare il loro Sistema di gestione della sicurezza delle informazioni (SGSI) nei processi strategici, creare efficienze e ottenere un maggiore coinvolgimento da parte della dirigenza.

Alcuni dei concetti principali dello standard ISO/IEC 27001:2013 sono:

Concetto	Commento
Contesto dell'organizzazione	Considera la combinazione di fattori interni ed esterni e le condizioni che possono influire sulle informazioni dell'organizzazione.
Aspetti, rischi e opportunità	Gli aspetti possono essere interni o esterni, positivi o negativi e riguardare condizioni che influiscono sulla riservatezza, sull'integrità e sulla disponibilità delle informazioni di un'organizzazione. I rischi sono definiti come "l'effetto dell'incertezza su un risultato previsto".
Parti interessate	Una persona o un'entità che possa influenzare, essere influenzata da, o percepirsi come influenzata da una decisione o un'attività. Ne sono un esempio i fornitori, i clienti o i concorrenti.
Leadership	Requisiti specifici della dirigenza intesa come una persona o un gruppo di persone che dirige e controlla un'organizzazione ai massimi livelli.
Rischio associato alle minacce e alle opportunità	Un processo di pianificazione accurato sostituisce un'azione preventiva ed è definito come 'l'effetto dell'incertezza su un risultato previsto'.
Comunicazione	Lo standard contiene requisiti espliciti e dettagliati sia per le comunicazioni interne che per quelle esterne.
Informazioni documentate	Dati o informazioni importanti che controllate o mantenete a supporto dell'SGSI.
Valutazione delle prestazioni	La misurazione dell'SGSI e dell'efficacia del piano di trattamento del rischio.
Proprietario del rischio (Risk Owner)	La persona o l'entità a cui è stata affidata l'autorità di gestire un particolare rischio di cui è responsabile.
Pianto di trattamento del rischio	Un piano di modifica del rischio che coinvolge la selezione e l'implementazione di una o più opzioni di trattamento rispetto a un rischio.
Controlli	Qualsiasi metodo amministrativo, gestionale, tecnico o legale che venga utilizzato per modificare o gestire un rischio di sicurezza delle informazioni. Possono comprendere pratiche, processi, politiche, procedure, programmi, strumenti, tecniche, tecnologie, dispositivi e strutture organizzative. Vengono stabiliti durante il processo di trattamento del rischio.
Miglioramento continuo	Possono essere impiegate altre metodologie oltre al ciclo Plan-Do-Check-Act (PDCA) (Pianifica-Esegui-Controlla-Agisci).



Requisiti chiave di ISO/IEC 27001:2013

Clause 1: Ambito

La prima clause descrive in dettaglio l'ambito dello standard.

Clause 2: Riferimenti normativi

Tutti i riferimenti normativi sono contenuti nello standard ISO/IEC 27000, Tecnologia delle informazioni – Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni – Panoramica e terminologia, a cui si fa riferimento e che fornisce un'utile guida.

Clause 3: Termini e definizioni

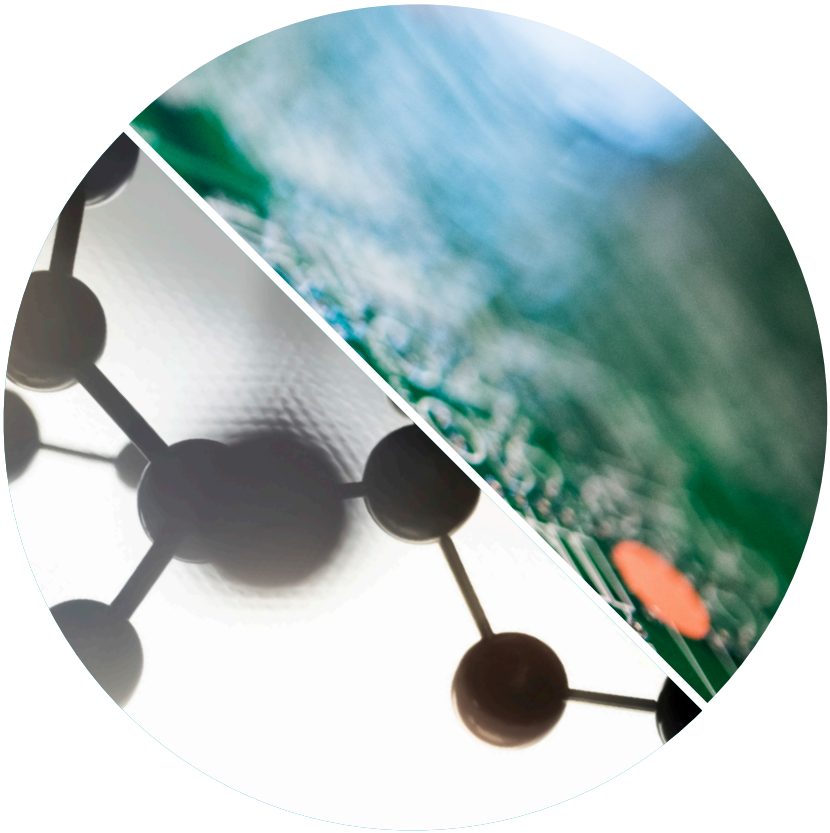
Fare riferimento ai termini e alle definizioni contenuti nello standard ISO/IEC 27000. È un documento importante da leggere.

Clause 4: Contesto dell'organizzazione

È la clause che stabilisce il contesto dell'organizzazione e gli effetti sull'SGSI. Gran parte dello standard si riferisce a questa clause.
Il punto di partenza consiste nell'identificare tutti gli aspetti esterni ed interni riguardanti la vostra organizzazione e le vostre informazioni o le informazioni che vi vengono affidate da terze parti. Dovete quindi stabilire quali siano le "parti interessate" e gli stakeholder, nonché in quale misura siano rilevanti ai fini delle informazioni.
Dovrete identificare i requisiti delle parti interessate, che potrebbero includere gli obblighi legali, di regolamentazione e/o contrattuali. Dovrete inoltre considerare argomenti importanti, come gli obiettivi di assicurazione e governance sul mercato. Dovrete decidere la portata del vostro SGSI, che deve essere compatibile con la direzione strategica della vostra organizzazione, con gli obiettivi chiave e i requisiti delle parti interessate.
E infine, dovrete mostrare come definite, implementate, mantenete e migliorate continuamente l'SGSI in relazione allo standard.

Clause 5: Leadership

Questa clause riguarda il ruolo della "dirigenza", ovvero il gruppo di persone che dirige e controlla la vostra organizzazione ai massimi livelli. Deve dimostrare leadership e impegno nell'espletamento delle proprie funzioni.
La dirigenza deve definire l'SGSI e la politica di sicurezza delle informazioni, assicurando che siano compatibili con la direzione strategica dell'organizzazione. Deve inoltre assicurarsi che siano resi disponibili, comunicati, mantenuti e compresi da tutte le parti..
La dirigenza deve assicurare il miglioramento continuo dell'SGSI, nonché l'orientamento e il supporto. Può assegnare all'SGSI le responsabilità e le autorità, ma continua comunque a esserne responsabile.



Clause 6: Pianificazione

Questa clause illustra il modo in cui un'organizzazione pianifica le azioni per far fronte ai rischi e alle opportunità delle informazioni.

Si focalizza sul modo in cui un'organizzazione gestisce il rischio di sicurezza delle informazioni affinché questo sia proporzionale al potenziale impatto. ISO 31000, lo standard internazionale per la gestione del rischio, contiene un'utile guida. Le organizzazioni sono inoltre tenute a produrre una "Dichiarazione di applicabilità" (Statement of Applicability, SoA). La SoA fornisce una sintesi delle decisioni che un'organizzazione ha preso in merito al trattamento del rischio, agli obiettivi di controllo e ai controlli che sono stati inclusi ed esclusi, nonché al motivo per cui è stato deciso di includere ed escludere i controlli nella SoA.

Un'altra area chiave di questa clause è la necessità di stabilire gli obiettivi della sicurezza delle informazioni e lo standard definisce le proprietà che gli obiettivi della sicurezza delle informazioni devono possedere.

Clause 7: Supporto

Questa sezione dello standard ISO/IEC 27001 riguarda l'impiego delle risorse, delle persone e delle infrastrutture idonee al fine di stabilire, implementare, mantenere e migliorare continuamente l'SGSI. Tratta i requisiti della competenza, della consapevolezza e delle comunicazioni a supporto dell'SGSI, ad esempio, rendendo disponibili attività formative e personale. Questa clause richiede inoltre che tutto il personale facente capo a un'organizzazione sia a conoscenza della politica di sicurezza delle informazioni, sia consapevole del proprio contributo alla sua efficacia e delle implicazioni qualora non la rispetti. L'organizzazione deve inoltre assicurarsi che le comunicazioni interne ed esterne pertinenti alla sicurezza delle informazioni e all'SGSI siano notificate in modo appropriato, ivi inclusa l'identificazione dell'oggetto della comunicazione, del destinatario, della data e della modalità con cui viene inviata.
È in questa clause che si fa riferimento al termine "informazioni documentate". Le organizzazioni devono determinare il livello di informazioni documentate necessario per controllare l'SGSI. It's in this clause that the term "documented information" is referenced. Organizations need to determine the level of documented information that's necessary to control the ISMS. Viene inoltre posto l'accento sul controllo dell'accesso alle informazioni documentate, il che riflette l'importanza della sicurezza delle informazioni

Clause 8: Attività operative

Questa clause riguarda l'attuazione dei piani e dei processi oggetto delle clausole precedenti. Descrive l'attuazione delle azioni determinate e il conseguimento degli obiettivi della sicurezza delle informazioni. Se si considera un maggiore ricorso alle funzioni esternalizzate nell'attuale mondo imprenditoriale, anche questi processi devono essere identificati e controllati. Qualsiasi cambiamento, sia esso pianificato o involontario, deve essere considerato in questa sede, oltre alle relative conseguenze sull'SGSI.
Ha inoltre per oggetto le prestazioni relative alle valutazioni sul rischio di sicurezza delle informazioni a intervalli pianificati, e l'esigenza di archiviare le informazioni documentate per registrare i risultati.
Infine, è presente una sezione che riguarda l'implementazione del piano di trattamento del rischio e, nuovamente, l'esigenza di archiviazione dei risultati nelle informazioni documentate.

Clause 9: Valutazione delle prestazioni

Questa clause riguarda il monitoraggio, la misurazione, l'analisi e la valutazione del vostro SGSI per garantirne l'efficacia nel tempo. Aiuta le organizzazioni a valutare continuamente il proprio comportamento in relazione agli obiettivi dello standard ai fini del miglioramento continuo. Dovrete considerare quali informazioni siano necessarie per valutare l'efficacia della sicurezza delle informazioni, i metodi impiegati e il momento in cui debbano essere analizzate e riportate.
Dovranno essere effettuati gli audit interni, oltre alle revisioni della gestione. Entrambi devono essere effettuati a intervalli pianificati, e i risultati dovranno essere archiviati come informazioni documentate. Va osservato che anche le revisioni della gestione sono un'opportunità per identificare le aree di miglioramento.

Clause 10: Miglioramento

Questa parte dello standard riguarda i requisiti delle azioni correttive. Dovrete documentare il modo in cui vengono gestite e risolte le non conformità, adottati provvedimenti e gestite le conseguenze. Dovrete inoltre mostrare se esistono eventuali non conformità analoghe o potrebbero potenzialmente verificarsi, e come eliminerete le cause in modo che non si verifichino in altri ambiti.
Siete inoltre tenuti a mostrare il miglioramento continuo dell'SGSI, inclusa la dimostrazione della idoneità e dell'adeguatezza e in quale misura sia efficace. Il modo in cui eseguire tali operazioni resta a vostra discrezione.
Lo standard ISO/IEC 27001 include anche l'Allegato A che delinea 114 controlli per aiutare a proteggere le informazioni in molteplici aree dell'organizzazione. Fornisce inoltre una guida per le migliori pratiche e rappresenta un valido riferimento per valutare quali controlli siano più adatti alla vostra organizzazione.

Come rendere efficace lo standard **ISO/IEC 27001** per la tua azienda

Ogni anno aiutiamo decine di migliaia di clienti. Di seguito vengono riportati alcuni consigli.

L'impegno della dirigenza è fondamentale ai fini del successo dell'implementazione dello standard ISO/IEC 27001. Deve essere coinvolta attivamente e approvare le risorse richieste.

"Prima le organizzazioni parlano con i vertici dirigenziali, meglio sarà per loro, dunque parlatene in fase preliminare".

John Scott, Overbury, azienda di allestimenti e ristrutturazioni leader nel Regno Unito

Organizza la **collaborazione tra i diversi repa**rti per evitare che lavorino a compartimenti stagni. Assicurati che l'organizzazione lavori in team a vantaggio dei clienti e dell'organizzazione.

"La chiave per l'implementazione dello standard sta nel convincere il personale a pensare alla sicurezza delle informazioni come parte integrante dell'attività quotidiana e non come un onere supplementare".

Mr. Thamer, Ibrahim Ali Arab, Assistant General

Revisiona i sistemi, le politiche, le procedure e i processi di cui dispone l'azienda: puoi già fare gran parte di quanto è contenuto nello standard, e farlo funzionare per la tua attività. Non dovresti agire solo ai fini dello standard. Lo standard deve aggiungere valore.

"Non cercare di cambiare la tua attività per adattarla alla norma. Pensa a come fai le diverse attività e a come lo standard si rifletta su di esse piuttosto che il contrario".

Paul Brazier, Commercial Director, Overbury

Parla con i clienti e fornitori. Potrebbero suggerirvi dei miglioramenti e darvi un feedback sul vostro servizio.

"Questa certificazione ci permette di fare un passo avanti, offrendo ai nostri clienti la certezza che abbiamo i migliori controlli in atto per individuare e ridurre i rischi per le informazioni riservate".

Jitesh Bavisi, Director of Compliance, Exponential-eBavisi

Forma il personale per effettuare gli audit interni del sistema. Ciò può favorire la comprensione, ma potrebbe anche fornire un prezioso feedback su potenziali problemi od opportunità per il conseguimento dei risultati.

"Il corso è ricco di esercizi pratici e di scenari reali ed è stato strutturato in modo da incoraggiare i partecipanti a essere interattivi e condividere le loro esperienze sulla sicurezza delle informazioni".

Nataliya Stephenson Manager, Information Security, NSW Attorney General's Department

E infine, una volta ottenuta la certificazione, celebra il traguardo e utilizza il marchio di conformità **BSI Assurance Mark** sulle pubblicazioni, sul sito web e sul materiale promozionale.

Il tuo percorso verso ISO/IEC 27001:2013

Se la tua organizzazione si sta avvicinando per la prima volta alla gestione della sicurezza delle informazioni o se sta cercando di migliorare il sistema di gestione esistente ti possiamo fornire risorse e corsi di formazione adeguati per aiutarti a capire e implementare lo standard ISO/IEC 27001:2013. Il nostro aiuto però non si ferma qui:

	Hai bisogno di:	Noi ti aiutiamo:
Capire e prepararsi	• Acquistare e leggere lo standard; comprenderne il contenuto, analizzare le tue esigenze e scoprire come potrà migliorare la tua attività • Contattarci, ti possiamo proporre la soluzione su misura per la tua organizzazione	• Acquista lo standard su BSI Shop Online • Scopri le informazioni all'interno del nostro sito web, compresi i whitepaper e webinar. Visita il nostro sito **bsigroup.it** • Corso di formazione ISO/IEC 27001:2013 Requirements di BSI
Scoprire quanto si è pronti	• Assicurarti che la tua organizzazione capisca i principi di ISO/IEC 27001:2013, i ruoli che i singoli soggetti dovranno ricoprire e rivedere le attività e le procedure che sono in conflitto con lo standard	• ISO/IEC 27001:2013 checklist di autovalutazione • Corso di formazione ISO/IEC 27001:2013 Implementing di BSI • Prenota un gap assessment con BSI per capire il grado di preparazione della tua organizzazione • Il BSI Business Improvement Software aiuta l'implementazione dello standard ISO/IEC 27001:2013
Valutazione e certificazione	• Contattarci per fissare la tua visita di certificazione • Assicurarti che tutte le persone giuste siano disponibili e pronte per la visita di controllo Questo è un processo che si divide in due fasi: la durata varia in base alle dimensioni della tua organizzazione	• Corsi di formazione ISO/IEC 27001:2013 Internal e Lead Auditor • BSI Business Improvement software consente di gestire in modo efficace il tuo sistema • Valutazione del sistema di gestione per la certificazione BSI

Miglioramento continuo e ricerca dell'eccellenza

Il percorso non si ferma alla certificazione. Possiamo aiutarvi a perfezionare la vostra organizzazione in modo che possa avere performance migliori

- Celebra e promuovi il raggiungimento della certificazione – scarica e utilizza il marchio di garanzia BSI, simbolo di eccellenza.
- Il tuo BSI Excellerator Report ti permetterà di confrontare le prestazioni della tua attività rispetto al settore di riferimento ed evidenzierà gli ambiti di miglioramento.
- Prenota un corso di formazione ISO/IEC 27001:2013 con BSI per implementare le tue conoscenze.
- Business Improvement Software di BSI ti aiuterà a gestire i sistemi e a garantirne le performance.
- Il tuo BSI Client Manager ti farà visita regolarmente per essere sicuro che la tua organizzazione sia conforme con lo standard e per supportarti verso un continuo miglioramento.

La Training Academy di BSI

Sfrutta la nostra competenza per ampliare le tue conoscenze: BSI vanta un portfolio completo di corsi di formazione a supporto dell'implementazione dello standard ISO/IEC 27001 e aiuta a sviluppare le competenze nell'organizzazione. I nostri docenti qualificati possono trasferire le conoscenze, le competenze e gli strumenti di cui ha bisogno il tuo personale per incorporare gli standard di eccellenza nell'organizzazione. Le tecniche di apprendimento accelerate applicate ai nostri corsi rafforzeranno inoltre il mantenimento delle conoscenze acquisite.

I corsi che aiutano a comprendere lo standard ISO/IEC 27001 includono:

Requirements ISO/IEC 27001:2013

- Corso in aula della durata di un giorno
- Apprendi la struttura e i requisiti chiave dello standard ISO/IEC 27001:2013
- Essenziale per chiunque sia coinvolto nelle fasi di pianificazione, implementazione, mantenimento, supervisione o audit di un SGSI conforme allo standard ISO/IEC 27001:2013

Internal Auditor ISO/IEC 27001:2013

- Corso in aula della durata di due giorni
- Scopri come intraprendere un audit, preparare e condurre le attività per un audit, compilare e distribuire i report dell'audit e completare le attività di follow-up
- Ideale per chiunque sia coinvolto nelle fasi di audit, mantenimento o supervisione di un SGSI conforme allo standard ISO/IEC 27001:2013

Implementazione dello standard ISO/IEC 27001:2013 di BSI

- Corso in aula della durata di tre giorni
- Scopri gli stadi dell'implementazione e la modalità di applicazione di un tipico framework per l'implementazione dello standard ISO/ IEC 27001
- Consigliato a chiunque sia coinvolto nelle fasi di pianificazione, implementazione, mantenimento o supervisione o audit di un SGSI conforme allo standard ISO/IEC 27001

Lead Auditor (revisore principale) di ISO/IEC 27001:2013

- Corso in aula della durata di cinque giorni
- Acquisisci le competenze e le conoscenze necessarie per condurre e intraprendere con successo un audit del sistema di gestione
- Consigliato a chiunque sia coinvolto nelle fasi di audit, mantenimento o supervisione di un SGSI conforme allo standard ISO/IEC 27001:2013.

Lead Implementer (realizzatore principale) di ISO/IEC 27001:2013

- Corso in aula della durata di cinque giorni
- Impara a comprendere gli strumenti e le metodologie per condurre un'implementazione dello standard ISO/IEC 27001
- Consigliato a chiunque sia coinvolto nelle fasi di pianificazione, implementazione, mantenimento o supervisione o audit di un SGSI conforme allo standard ISO/IEC 27001

Business Improvement Software di BSI

Accelera i tempi d'implementazione e apporta miglioramenti continui

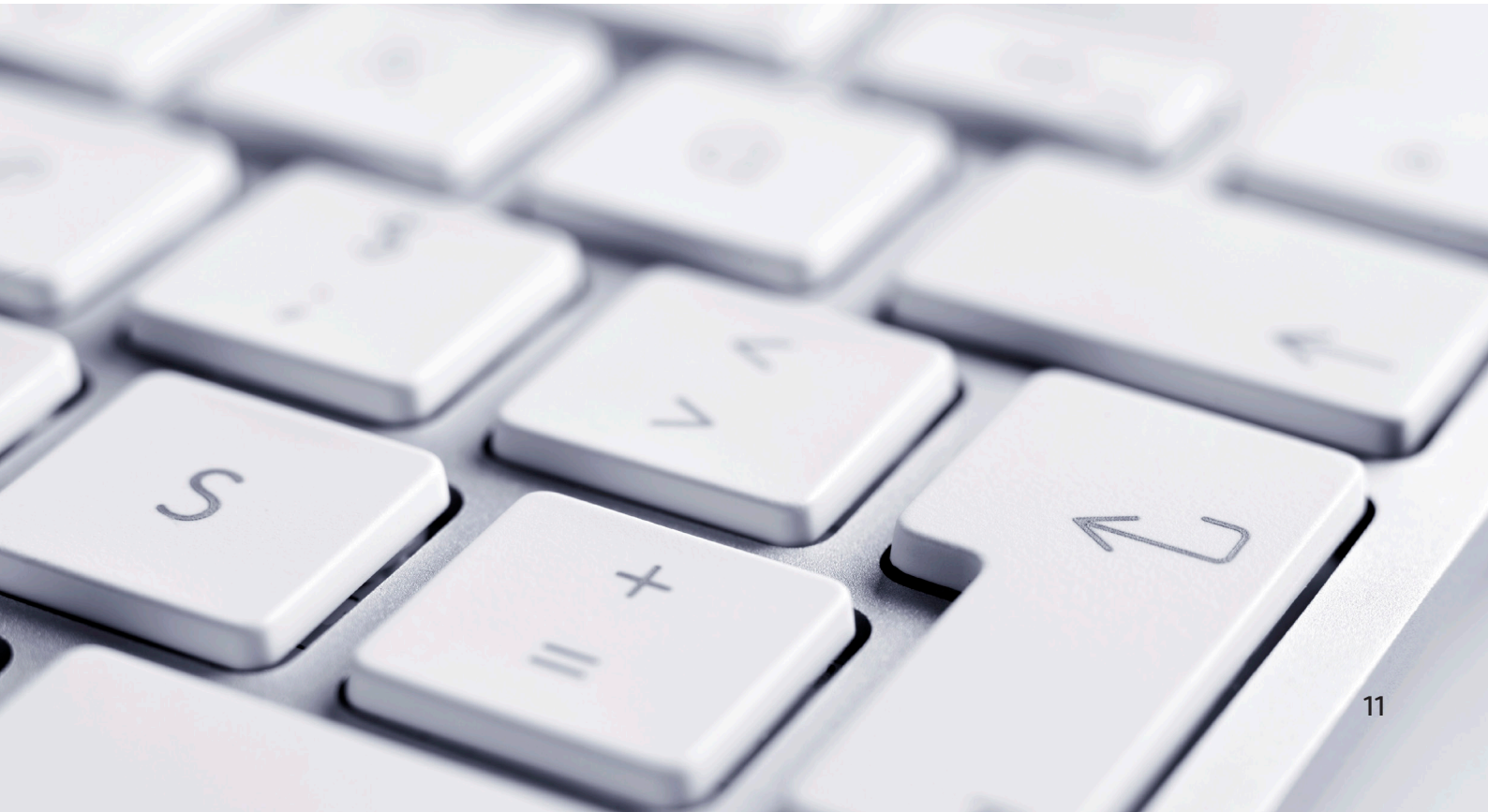
La decisione di implementare un nuovo standard del sistema di gestione è una straordinaria opportunità per conseguire miglioramenti aziendali, sebbene avviarlo, implementarlo e mantenerlo possa comportare anche una sfida. Avere la certezza di ottenere il massimo dal proprio investimento è uno dei principali motori per il successo futuro.

Il Business Improvement Software di BSI offre una soluzione per ridurre significativamente i costi e l'impegno per l'implementazione di un sistema di gestione efficace come lo standard ISO/IEC 27001. Può essere configurato in base ai requisiti dello standard ISO/IEC 27001 e fornire alla vostra organizzazione gli strumenti necessari per gestire gli elementi essenziali dello standard ISO/IEC 27001 nella vostra organizzazione. L'inizio del viaggio per la certificazione ISO/IEC 27001 è il momento ideale per implementare con successo il Business Improvement Software di BSI a supporto dello standard.

Può aiutarti a:

- Accelerare i tempi di implementazione fino al 50%
- Gestire efficacemente il controllo dei documenti
- Fornire visibilità a tutta l'azienda sull'implementazione dello standard in modo che sappiate sempre ed esattamente in quale fase si trova
- Elaborare azioni correlate ad audit, incidenti/eventi, rischi e prestazioni in maniera facile ed accurata
- Anticipare la comprensione degli andamenti tramite i dashboard personalizzabili e gli strumenti di reporting, aiutandovi a prendere decisioni in anticipo e ottenere miglioramenti

Grazie a una completa visibilità a livello di struttura, ora l'azienda è in grado di ottenere risparmi sui costi.



Perché BSI?

By Royal Charter

ISO/IEC 27001:2013 Information Security Management

BSI è stato in prima linea nella definizione di ISO/IEC 27001:2013, il primo standard per la sicurezza delle informazioni originariamente basato su BS 7799, sviluppato da BSI nel 1995. Abbiamo partecipato al suo sviluppo da quando è cominciata l'evoluzione dello standard ISO/IEC 27001:2013 ad oggi. Per questo motivo siamo nella posizione migliore per aiutarti a capirlo, implementarlo e trarre benefici dalla sua applicazione.
In BSI creiamo eccellenza, portando i nostri clienti al successo attraverso gli standard. Aiutiamo le organizzazioni a diventare resilienti, le supportiamo perchè possano crescere in maniera sostenibile, a diventare adattabili al cambiamento e mantenere il successo nel lungo periodo.
"*We make excellence a habit*".
Da oltre un secolo i nostri esperti combattono la mediocrità e l'indifferenza per aiutare a portare l'eccellenza sia nelle persone sia nei prodotti. Con 80.000 clienti in 182 paesi, BSI è un'organizzazione i cui standard ispirano l'eccellenza in tutto il mondo.

I nostri prodotti e servizi

Forniamo una combinazione unica di prodotti e servizi complementari, gestiti attraverso tre aree di competenza: conoscenza, garanzia e conformità.

Conoscenza

Il cuore della nostra attività si basa sulla conoscenza che creaiamo e trasmettiamo ai nostri clienti. Continuiamo a costruire la nostra reputazione nel campo degli standard in qualità di organo specializzato; riuniamo esperti di settore per dare vita a standard a livello locale, regionale e internazionale. BSI ha infatti creato, in origine, otto dei primi 10 standard sui sistemi di gestione a livello mondiale.

Garanzia

Valutazione indipendente della conformità, di un processo o di prodotto, ad un particolare standard per garantire ai nostri clienti performance caratterizzate da un alto livello di eccellenza. Formiamo i nostri clienti con tecniche consolidate a livello mondiale per garantire che ottengano tutti i benefici derivanti dai nostri standard.

Conformità

Per sperimentare benefici reali a lungo termine, i nostri clienti devono assicurarsi una conformità permanente ai regolamenti, alle esigenze del mercato o agli standard, e fare in modo che questa diventi un'attitudine aziendale. Forniamo servizi di consulenza e strumenti di gestione differenziati al fine di facilitare tale procedura.

bsi.

marketing.italy@bsigroup.com
Call: +39 02 6679091
Visit: bsigroup.it