ISO/IEC 27001:2013

Questionario di autovalutazione

Quanto pronti siete?

Questo documento è stato concepito per valutare in quale misura la vostra azienda è pronta per una valutazione della certificazione del Sistema di gestione della sicurezza delle informazioni (Information Security Management System, ISMS) ISO/IEC 27001:2013. Compilando il presente questionario sarete in grado di valutare la vostra organizzazione e identificare il vostro livello di preparazione per quanto concerne i principali requisiti dello standard.

Contesto dell'organizzazione

- Avete identificato i problemi esterni e interni rilevanti ai fini della vostra organizzazione e che incidono sulla vostra capacità di raggiungere i risultati attesi nell'ambito del vostro sistema di gestione della sicurezza delle informazioni (SGSI)?
- Avete un sistema per rivedere e monitorare con regolarità tali problemi e la loro evoluzione?
- Avete identificato esigenze e aspettative per le parti interessate pertinenti ai fini dell'SGSI e, in caso affermativo, le esaminate periodicamente?
- Avete determinato l'ambito del vostro SGSI e avete tenuto conto dei problemi esterni e interni, delle parti interessate e di eventuali attività svolte da altre organizzazioni?
- Sono stati valutati i problemi interni ed esterni che potrebbero ripercuotersi sul sistema SGSI?
- Siete consapevoli delle esigenze delle parti interessate, quali i requisiti legali e normativi nonché quelli dei vostri clienti?
- Sono stati considerati i rischi e le opportunità associati a tali problemi e requisiti?
- È stato preso in considerazione il miglioramento continuo?

Leadership

- I vertici aziendali si sono assunti la responsabilità dell'efficacia dell'SGSI e hanno trasmesso l'importanza di un SGSI efficace in azienda?
- La policy e gli obiettivi dell'SGSI, compatibili con il contesto e la direzione strategica dell'organizzazione, sono stati definiti e comunicati?
- Nell'ambito dell'SGSI i ruoli sono stati designati, trascritti e comunicati con chiarezza?
- I ruoli hanno l'autorità per garantire la conformità e il reporting, nonché la responsabilità?

Continued >>

Leadership – *continued*

È stato sviluppato e adottato un programma per garantire che l'SGSI raggiunga risultati, requisiti e obiettivi definiti?

Pianificazione

Sono stati identificati rischi e opportunità con cui ci si dovrà misurare per garantire che l'SGSI possa raggiungere i risultati attesi?

È stato istituito un processo di valutazione del rischio per la sicurezza delle informazioni che comprenda criteri di accettazione dei rischi?

Il processo di valutazione del rischio per la sicurezza delle informazioni è stato sviluppato in modo da essere ripetibile?

Produce risultati coerenti, validi e comparabili?

L'organizzazione ha pianificato e integrato azioni per affrontare tali rischi e opportunità?

Il processo di valutazione del rischio per la sicurezza delle informazioni è in grado di identificare i rischi associati alla perdita di riservatezza, integrità e disponibilità delle informazioni nell'ambito dell'SGSI?

Sono stati identificati i titolari dei rischi?

Sono stati analizzati i rischi per la sicurezza delle informazioni per valutarne la probabilità realistica e le potenziali conseguenze che ne deriverebbero, qualora si verificassero, e sono stati determinati i livelli di rischio?

I rischi per la sicurezza delle informazioni sono stati valutati sulla base dei criteri di rischio accertati e classificati in ordine di priorità?

Le informazioni sul processo di valutazione del rischio per la sicurezza delle informazioni sono documentate e disponibili?

Il processo di trattamento del rischio per la sicurezza delle informazioni consente opzioni appropriate?

Sono stati determinati controlli per attuare l'opzione scelta di trattamento del rischio?

I controlli determinati sono stati confrontati con ISO/IEC 27001:2013, allegato A, per verificare che non siano stati omessi i controlli necessari?

Avete prodotto una dichiarazione di applicabilità per giustificare le esclusioni e le inclusioni di cui all'allegato A, insieme allo stato di attuazione dei controlli?

È stato creato un piano di trattamento del rischio per la sicurezza delle informazioni?

- I titolari del rischio hanno esaminato e approvato il piano?
- I rischi residui per la sicurezza delle informazioni sono stati autorizzati dai titolari del rischio?
- È documentato?

Pianificazione – *continued*

Esiste un piano per determinare la necessità di modifiche all'SGSI e per gestirne l'attuazione?

Obiettivi e traguardi misurabili dell'SGSI sono stati definiti, documentati e trasmessi in tutta l'organizzazione?

Nel fissare i propri obiettivi, l'organizzazione ha indicato quali misure sia necessario intraprendere, la tempistica e i responsabili?

Support

L'organizzazione ha determinato e fornito le risorse necessarie per l'istituzione, l'attuazione, il mantenimento e il miglioramento continuo dell'SGSI (comprese persone, infrastrutture e ambiente per l'esercizio dei processi)?

Esiste un processo definito e documentato per determinare le competenze dei ruoli nell'ambito dell'SGSI?

- Questo processo e le competenze di coloro che ricoprono tali ruoli sono documentati?

L'organizzazione ha determinato le conoscenze indispensabili per coloro che svolgono ruoli nell'ambito dell'SGSI?

L'organizzazione si è accertata che le persone in grado di influire su prestazioni ed efficacia dell'SGSI siano competenti sulla base di un'adeguata istruzione, formazione o esperienza oppure ha intrapreso misure atte a garantire che tali persone possano acquisire le competenze necessarie?

Le informazioni documentate richieste dallo standard e indispensabili per l'efficace attuazione ed esercizio del sistema SGSI sono state determinate?

Le informazioni documentate sono controllate affinché siano disponibili e adeguatamente protette, distribuite, archiviate, conservate e sottoposte al controllo delle modifiche, inclusi i documenti di origine esterna richiesti dall'organizzazione per l'SGSI?

Operation

Sono state conservate prove documentate per dimostrare che i processi sono stati eseguiti come pianificato?

Esiste un piano per determinare la necessità di modifiche all'SGSI e per gestirne l'attuazione?

Quando sono previste modifiche, queste vengono effettuate in modo controllato e vengono intraprese azioni per mitigare eventuali effetti negativi?

Se esistono processi in outsourcing, questi sono opportunamente controllati?

Continued >>

Operation – *continued*

Le valutazioni del rischio per la sicurezza delle informazioni vengono svolte a intervalli pianificati o quando si verificano cambiamenti significativi, e vengono conservate informazioni documentate?

L'organizzazione ha pianificato azioni per affrontare rischi e opportunità e le integra nei processi del sistema?

Queste azioni sono documentate?

Valutazione delle prestazioni

Disponete di criteri per la valutazione, la selezione, il monitoraggio delle prestazioni e la rivalutazione dei vostri fornitori esterni?

Avete determinato che cosa debba essere monitorato e misurato, la tempistica, i responsabili, i metodi da utilizzare e quando saranno valutati i risultati?

I risultati del monitoraggio e delle misurazioni sono documentati?

Vengono condotti periodicamente audit interni per verificare che l'SGSI sia efficace e conforme da un lato allo standard ISO/IEC 27001:2013 dall'altro alle esigenze dell'organizzazione?

L'organizzazione ha istituito un programma per gli audit interni dell'SGSI?

I risultati degli audit sono comunicati alla direzione, documentati e conservati?

Se vengono identificate non conformità, l'organizzazione ha istituito gli opportuni processi per gestirle e le rispettive azioni correttive?

I vertici aziendali effettuano revisioni regolari e periodiche dell'SGSI?

L'esito della revisione della gestione dell'SGSI identifica modifiche e miglioramenti?

Performance eveluation – *continued*

I risultati della revisione della gestione sono documentati, tradotti in pratica e comunicati alle parti interessate, secondo i casi?

Se vengono identificate non conformità, l'organizzazione ha messo in atto gli opportuni processi per gestirle e le rispettive azioni correttive?

I vertici aziendali intraprendono revisioni regolari e periodiche dell'SGSI?

L'esito della revisione della gestione dell'SGSI identifica modifiche e miglioramenti?

I risultati della revisione della gestione sono documentati, tradotti in pratica e comunicati alle parti interessate, secondo i casi?

Miglioramento

Sono state individuate azioni per controllare, correggere e gestire le conseguenze di non conformità?

È stata valutata la necessità di intervenire per eliminare la causa principale delle non conformità onde evitare che si ripetano?

Le eventuali azioni correttive individuate sono state messe in atto e riviste per verificarne l'efficacia dando così luogo a miglioramenti dell'SGSI?

Vengono conservate informazioni documentate a testimonianza della natura delle non conformità, delle azioni intraprese e dei risultati?

BSI/UK/820/SC/0316/EN/BLD