Cybersecurity

Topical Requirement

Requisito Tematico

The Institute of
Internal Auditors

Requisito Tematico sulla cybersecurity

L'International Professional Practices Framework® comprende i Global Internal Audit Standards™, i Requisiti Tematici e le Global Guidance. I Requisiti Tematici sono una componente obbligatoria e devono essere utilizzati insieme ai Global Internal Audit Standards, che costituiscono la base autorevole delle pratiche di audit richieste.

I Requisiti Tematici forniscono chiare indicazioni per gli Internal Auditor, stabilendo un livello minimo di riferimento per gli incarichi di audit aventi ad oggetto specifici rischi. Il profilo di rischio specifico dell'organizzazione potrebbe richiedere agli Internal Auditor di considerare ulteriori aspetti dell'argomento in questione.

La conformità ai Requisiti Tematici aumenterà la coerenza con cui vengono svolti i servizi di Internal Auditing e migliorerà la qualità e l'affidabilità degli incarichi di audit e dei risultati. In definitiva, i Requisiti Tematici elevano la professione di Internal Auditing.

Gli Internal Auditor devono applicare i Requisiti Tematici in conformità con i Global Internal Audit Standard. La conformità ai Requisiti Tematici è obbligatoria per i servizi di assurance e raccomandata per i servizi di advisory.

Il Requisito Tematico si applica quando l'argomento è:

A. Oggetto di un incarico di audit incluso nel piano di Audit.
B. Identificato durante l'esecuzione di un incarico.
C. Oggetto di una richiesta di incarico non prevista nel piano di Audit originale.

Deve essere tenuta traccia e conservata la documentazione a supporto dell'applicabilità di ciascun requisito previsto dal Requisito Tematico. Non tutti i singoli requisiti possono applicarsi ad ogni incarico di audit; se vi sono requisiti esclusi è necessario documentarne la motivazione e conservarne evidenza. La conformità ai Requisiti Tematici è obbligatoria e sarà valutata durante i processi di quality assessment.

Per ulteriori informazioni, consultare la User Guide sul Requisito Tematico sulla cybersecurity.

Cybersecurity

Il National Institute of Standards and Technology (NIST) definisce la cybersecurity semplicemente come "*la capacità di proteggere o difendere l'uso del cyberspazio da attacchi informatici*". La cybersecurity è un sottoinsieme della sicurezza delle informazioni, che il NIST definisce come "*la protezione delle informazioni e dei sistemi informativi da accessi, utilizzi,*

divulgazioni, interruzioni, modifiche o distruzioni non autorizzati, al fine di garantirne la riservatezza, integrità e disponibilità".

La cybersecurity riduce il rischio rafforzando l'ambiente di controllo complessivo e proteggendo gli asset informativi di un'organizzazione da accessi non autorizzati, interruzioni, alterazioni o distruzioni. Gli attacchi informatici possono avere impatti diretti e indiretti spesso significativi, poiché computer, reti, programmi, dati e informazioni sensibili rappresentano componenti critici per la maggior parte delle organizzazioni.

Valutazione e verifica dei processi di Governance, Risk Management e Controllo della Cybersecurity

Questo Requisito Tematico fornisce un approccio coerente e completo per valutare la progettazione e l'implementazione dei processi di governance, risk management e controllo della cybersecurity. I requisiti rappresentano una base minima per la valutazione della cybersecurity all'interno di un'organizzazione.

GOVERNANCE: Valutare e verificare la governance della cybersecurity

Requisiti:

Gli Internal Auditor devono valutare i seguenti aspetti in relazione alla governance della cybersecurity dell'organizzazione:

- **A.** Una strategia di cybersecurity e i relativi obiettivi sono definiti e aggiornati periodicamente. Gli aggiornamenti sul raggiungimento di tali obiettivi sono comunicati e riesaminati periodicamente dal Board, includendo considerazioni relative alle risorse e al budget necessari per supportare la strategia di cybersecurity.
- **B.** Le policy e le procedure in materia di cybersecurity sono definite e aggiornate regolarmente per rafforzare l'ambiente di controllo.
- **C.** I ruoli e le responsabilità a supporto degli obiettivi di cybersecurity sono chiaramente definiti ed esiste un processo per valutare periodicamente le conoscenze, le competenze e le capacità delle persone che esercitano tali ruoli.
- **D.** Gli stakeholder devono essere coinvolti per discutere e affrontare le vulnerabilità esistenti e le minacce emergenti nel contesto della cybersecurity.Tra gli stakeholder rientrano il Top Management, le Funzioni Operative, il Risk Management, le Risorse Umane, l'Ufficio Legale, la Compliance, i fornitori e altri soggetti rilevanti.

RISK MANAGEMENT: Valutare e verificare il risk management della cybersecurity

Requisiti:

Gli Internal Auditor devono valutare i seguenti aspetti in relazione al risk management della cybersecurity dell'organizzazione:

A. I processi di risk assessment e risk management dell'organizzazione includono l'identificazione, l'analisi, la mitigazione e il monitoraggio delle minacce informatiche e del loro impatto sul raggiungimento degli obiettivi strategici.

B. Il risk management sulla cybersecurity è condotto a livello aziendale e può includere le seguenti aree: Information Technology, Enterprise Risk Management, Risorse Umane, Area Legale, Compliance, Operations, Supply Chain, Contabilità, Finanza e altre funzioni.

C. Le responsabilità e gli incarichi sul risk management della cybersecurity sono definite. È individuata una persona o un team incaricato di monitorare periodicamente e riferire sulla gestione dei rischi di cybersecurity, comprese le risorse necessarie per mitigarli e l'identificazione delle minacce emergenti.

D. È stabilito un processo per segnalare tempestivamente qualsiasi rischio di cybersecurity (emergente o già identificato) che raggiunga un livello inaccettabile, in base alle linee guida risk management dell'organizzazione o ai requisiti legali e normativi applicabili. Dovrebbero essere presi in considerazione sia gli impatti finanziari che quelli non finanziari derivanti dai rischi di cybersecurity.

E. È stabilito un processo per sensibilizzare il management e i dipendenti sui rischi di cybersecurity e per consentire al management di riesaminare periodicamente problematiche, lacune, carenze o mancanze di controllo attraverso modalità tempestive di segnalazione e risoluzione.

F. L'organizzazione ha implementato un processo di gestione della risposta e ripristino in seguito ad incidenti di cybersecurity che comprende la rilevazione, il contenimento, il ripristino e l'analisi post-incidente. Il processo di risposta e ripristino dagli incidenti è sottoposto a test periodici.

CONTROLLI: Valutare e verificare i processi di controllo della cybersecurity

Requisiti:

Gli Internal Auditor devono valutare i seguenti aspetti in relazione ai processi di controllo della cybersecurity:

A. È stabilito un processo per garantire sia l'efficacia dei controlli interni all'organizzazione sia di quelli effettuati dai fornitori, al fine di proteggere la riservatezza, l'integrità e la disponibilità dei sistemi informativi e dei dati aziendali. Vengono effettuate valutazioni periodiche per verificare l'efficacia di tali controlli nel supportare il raggiungimento degli obiettivi di cybersecurity dell'organizzazione e nell'assicurare la tempestiva risoluzione delle problematiche.

B. È stabilito un processo di gestione dei talenti che include la formazione per sviluppare e aggiornare le competenze tecniche in ambito cybersecurity. Tale processo viene rivisto periodicamente.

C. È stabilito un processo per il monitoraggio continuo e per la segnalazione delle minacce e delle vulnerabilità emergenti e per identificare, prioritizzare e implementare opportunità di miglioramento in ambito cybersecurity.

D. La cybersecurity deve essere integrata nella gestione del ciclo di vita (selezione, utilizzo, mantenimento e dimissione) di tutte le risorse IT, inclusi hardware, software e servizi forniti da terze parti.

E. Sono definiti processi per rafforzare la cybersecurity che includono le configurazioni l'amministrazione dei dispositivi degli utenti finali, la crittografia, il patching, la gestione degli accessi e il monitoraggio della disponibilità e delle prestazioni. Le considerazioni sulla cybersecurity sono incluse nei processi di sviluppo software (DevSecOps).

F. Sono stabiliti controlli sulla sicurezza della rete come la segmentazione della rete e gestione degli accessi; l'uso e il posizionamento dei firewall; connessioni limitate da e verso reti esterne, Virtual Private Network (VPN) e modelli Zero Trust (ZTNA); controlli sulla rete dell'Internet of Things (IoT) e sistemi di rilevamento e prevenzione dalle intrusioni (IDS e IPS).

G. Sono definiti controlli di sicurezza per la comunicazione degli end-point nei servizi quali e-mail, browser internet, videoconferenze, messaggistica, social media, cloud e protocolli di condivisione file.

Informazioni sull'Istituto dei revisori interni

L'Institute of Internal Auditors (IIA) è un'associazione professionale internazionale che conta più di 255.000 membri a livello globale e ha rilasciato più di 200.000 certificazioni di Certified Internal Auditor® (CIA®) in tutto il mondo. Fondata nel 1941, l'IIA è riconosciuta in tutto il mondo come leader nella professione dell'internal audit per quanto riguarda gli standard, le certificazioni, la formazione, la ricerca e la guida tecnica. Per maggiori informazioni, visitate il sito www.theiia.org.

Copyright

Febbraio 2025

The Institute of Internal Auditors

Sede centrale globale
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Telefono: +1-407-937-1111
Fax: +1-407-937-1101