Cybersecurity

Topical Requirement

Requisito Tematico

User Guide

The Institute of
Internal Auditors

Contenuti

Introduzione ai Requisiti Tematici

I Requisiti Tematici sono un elemento essenziale dell'International Professional Practices Framework® (IPPF), insieme ai Global Internal Audit Standards™ e alle Global Guidance. L'Institute of Internal Auditors (IIA) richiede che i Requisiti Tematici siano utilizzati in combinazione con i Global Internal Audit Standards, che costituiscono la base autorevole per le pratiche di audit richieste. All'interno di questa guida sono presenti riferimenti agli Standards che forniscono informazioni più dettagliate.

I Requisiti Tematici definiscono un riferimento metodologico per guidare gli Internal Auditor nella gestione di specifici rischi garantendo la coerenza e la qualità delle attività di Internal Auditing. Essi stabiliscono una base di riferimento e forniscono criteri pertinenti (significativi) per l'esecuzione dei servizi di assurance relativi alla tematica trattata da un determinato Requisito (Standard 13.4 - Criteri di Valutazione). La conformità ai Requisiti Tematici è obbligatoria per i servizi di assurance e raccomandata per i servizi di advisory. Tuttavia, i requisiti non intendono coprire tutti gli aspetti potenzialmente rilevanti per un incarico di assurance, ma forniscono un insieme minimo di requisiti per garantire una valutazione coerente e affidabile dell'argomento trattato.

I Requisiti Tematici sono strettamente collegati al *Three Lines Model* dell'IIA e ai Global Internal Audit Standard. I processi di governance, risk management e controllo sono i principali componenti dei Requisiti Tematici, in linea con lo Standard 9.1 - Comprensione dei processi di governance, risk management e controllo. Nel *Three Lines Model*, la governance fa capo al Board o all'organo di governo, la gestione del rischio è affidata alla Seconda Linea, mentre i controlli operativi e i processi di controllo rientrano nella Prima Linea.

Nel *Three Lines Model*, la funzione Internal Audit è rappresentata come la Terza Linea, fornendo un'assicurazione indipendente e obiettiva al Board o all'organo direttivo mentre la Prima e la Seconda Linea coinvolge il management operativo. (Principio 8 Sottoposta alla supervisione del Board).

Applicabilità, rischio e giudizio professionale

I Requisiti Tematici devono essere applicati quando le funzioni Internal Audit svolgono incarichi di assurance su temi per i quali esiste un Requisito Tematico, oppure quando elementi di tale requisito emergono all'interno di altri incarichi di assurance.

Come descritto negli Standard, il risk assessment è un elemento fondamentale nella pianificazione del Chief Audit Executive (CAE). La definizione degli incarichi di assurance da includere nel piano di Audit richiede un'analisi periodica, almeno annuale, delle strategie, degli obiettivi e dei rischi dell'organizzazione (Standard 9.4 Piano di Audit). Nella pianificazione degli

incarichi di assurance, gli Internal Auditor devono valutare i rischi rilevanti per l'incarico (Standard 13.2 Risk assessment dell'incarico).

Se durante la pianificazione risk-based dell'Internal Auditing, viene identificato un argomento tra quelli oggetto di un Requisito Tematico e quindi inserito nel piano di Audit, è obbligatorio applicare i requisiti previsti nel Requisito Tematico in questione all'interno degli incarichi, ove applicabili. Inoltre, quando gli Internal Auditor svolgono un incarico (sia esso previsto o meno nel piano di Audit) e emergono elementi riconducibili a un Requisito Tematico, quest'ultimo deve essere valutato per determinare la sua applicabilità nell'ambito dell'incarico stesso. Infine, se viene richiesto un incarico non originariamente previsto nel piano di Audit, ma che riguarda un argomento coperto da un Requisito Tematico, è necessario valutarne l'applicabilità.

Il giudizio professionale dell'Internal Audit ha un ruolo fondamentale nell'applicazione del Requisito Tematico. Il risk assessment guida le decisioni del Chief Audit Executive riguardo gli incarichi da includere nel piano di Audit (Standard 9.4 - Piano di Audit). Inoltre, gli Internal Auditor applicano il giudizio professionale per determinare quali aspetti devono essere considerati all'interno di ciascun incarico (Standard 13.3 - Obiettivi e ambito dell'incarico, 13.4 Criteri di valutazione, 13.6 – Programma di lavoro). L'Appendice A "Esempi di applicazione pratica" fornisce indicazioni pratiche su come gli Internal Auditor determinano l'applicabilità di un Requisito Tematico.

Le evidenze relative alla valutazione dell'applicabilità di ciascun Requisito Tematico devono essere documentate, includendo una motivazione per eventuali esclusioni. La conformità ai Requisiti Tematici deve essere documentata secondo il giudizio professionale dell'Internal Audit, come previsto nello Standard 14.6 - Documentazione dell'incarico.

Sebbene il Requisito Tematico sulla Cybersecurity fornisca una base di riferimento per i processi di controllo da considerare, le organizzazioni che valutano il rischio cybersecurity come molto elevato potrebbero dover analizzare ulteriori aspetti.

Se il CAE constata che la funzione Internal Audit non possiede le competenze necessarie per svolgere incarichi di audit su un argomento specifico di un Requisito Tematico, l'incarico può essere esternalizzato (Standard 3.1 - Competenza, 7.2 – Qualifiche del Chief Audit Executive, 10.2 - Risorse Umane). Tuttavia, anche in caso di esternalizzazione, la funzione Internal Audit rimane comunque responsabile di garantire la conformità ai Requisiti Tematici, e il CAE ne mantiene la responsabilità ultima. Inoltre, se il CAE ritiene che le risorse interne siano insufficienti, deve informare il Board sugli impatti derivanti da questa carenza e su come affrontarla (Standard 8.2 - Risorse).

Performance, documentazione e reporting

Nell'applicare i Requisiti Tematici, gli Internal Auditor devono anche conformarsi agli Standard, svolgendo il loro lavoro in linea con la Sezione V: Svolgimento delle attività di Internal Auditing. Gli Standard della Sezione V descrivono le fasi chiave degli incarichi di Internal Audit, tra cui: la pianificazione degli incarichi (Standard 13 - Pianificare gli incarichi in modo efficace), la conduzione degli incarichi (Standard 14 - Condurre l'incarico) e la comunicazione dei risultati dell'incarico (Standard 15 - Comunicare i risultati dell'incarico e monitorare i piani d'azione).

La conformità ai Requisiti Tematici può essere documentata nel piano di Audit o nelle carte di lavoro dell'incarico, in base al giudizio professionale degli Internal Auditor. Uno o più incarichi di Internal Audit possono soddisfare il Requisito Tematico anche se non tutti potrebbero essere applicabili. È necessario conservare l'evidenza della valutazione dell'applicabilità del Requisito Tematico, compresa la motivazione delle eventuali esclusioni.

La tabella di cui all'Appendice C costituisce uno strumento opzionale utilizzabile come riferimento per documentare il lavoro svolto dagli Internal Auditor.

Quality Assurance

Gli Standard prevedono che il CAE sviluppi, attui e mantenga un programma di assurance e miglioramento della qualità che copra tutti gli aspetti della funzione Internal Audit (Standard 8.3 - Qualità). I risultati devono essere comunicati al Board e al Top Management. Le comunicazioni devono riportare la conformità della funzione Internal Audit agli Standard e il raggiungimento degli obiettivi di performance.

La conformità ai Requisiti Tematici sarà valutata nei quality assessment. Per prepararsi alla quality review, gli Internal Auditor possono utilizzare lo strumento fornito nell'Appendice C.

Cybersecurity

La cybersecurity è un tema ampio che coinvolge la maggior parte degli aspetti tecnologici di un'organizzazione. Oltre all'information technology, la cybersecurity è spesso integrata nei processi aziendali, rendendo fondamentale per gli Internal Auditor la valutazione dei rischi cyber nelle fasi di pianificazione, definizione dell'ambito e svolgimento degli incarichi di assurance.

Il National Institute of Standards and Technology (NIST), parte del Dipartimento del Commercio degli Stati Uniti, definisce la cybersecurity semplicemente come "*la capacità di proteggere o difendere l'uso del cyberspazio da attacchi informatici*". Il Requisito Tematico sulla cybersecurity si concentra sul perimetro esterno delle organizzazioni per mitigare i rischi derivanti da accessi non autorizzati e minacce informatiche. 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 garantire la riservatezza, integrità e disponibilità*".

I requisiti del Requisito Tematico sulla cybersecurity comprendono:

- Governance - definizione chiara di obiettivi e strategie di cybersecurity, in linea con le policy e le procedure organizzative.
- Risk Management - processi per identificare, analizzare, gestire e monitorare le minacce cyber, inclusa una procedura per l'escalation dei rischi cyber.

Controlli - definizione di processi di controllo, gestiti dal management e sottoposti a valutazioni periodiche per mitigare il rischio di cybersecurity.

Aspetti da valutare

Gli Internal Auditor possono utilizzare i seguenti aspetti per facilitare la valutazione dei requisiti previsti nel Requisito Tematico sulla cybersecurity. Questi aspetti, che rimandano ai requisiti, sono esemplificativi ma non obbligatori. Gli Internal Auditor devono affidarsi al giudizio professionale per determinare cosa includere nelle loro valutazioni.

Aspetti da valutare sulla governance

Per valutare l'applicazione dei processi di governance agli obiettivi di cybersecurity, gli Internal Auditor possono esaminare i seguenti aspetti:

A. Piano strategico e obiettivi di cybersecurity formalizzati e documentati, compresa l'evidenza che il Board esamini periodicamente (in genere trimestralmente) gli aggiornamenti sulla cybersecurity forniti dal responsabile della funzione di sicurezza informatica, come il Chief Information Security Officer (CISO). Le evidenze possono includere report su:
    - Monitoraggio del raggiungimento degli obiettivi strategici.
    - Esigenze di budget per sostenere gli obiettivi di cybersecurity.
    - Rischi e controlli interni, compreso l'avanzamento dei piani di remediation.
    - Key performance indicators (KPIs)
    - Risorse umane necessarie per l'assunzione, la formazione e lo sviluppo del personale dedicato alla cybersecurity.

B. Policy, procedure e altra documentazione adeguata a supporto dei processi di cybersecurity, tra cui:
    - Policy riviste e aggiornate almeno annualmente. I rischi di cybersecurity emergenti possono richiedere revisioni e aggiornamenti più frequenti.
    - Un processo per determinare se le policy e le procedure sono sufficienti a supportare le attività operative di cybersecurity.
    - Framework riconosciuti (NIST, COBIT e altri) per rafforzare i processi e i controlli in ambito cybersecurity.

C. Ruoli e responsabilità finalizzati al raggiungimento degli obiettivi di cybersecurity, con una struttura organizzativa che assicuri alla funzione cybersecurity un adeguato posizionamento e il necessario supporto da parte dell'organizzazione.
    - Un processo per valutare periodicamente le conoscenze, le competenze e le capacità del personale che ricopre ruoli in ambito cybersecurity.

D. Evidenze a supporto sul coinvolgimento dei principali stakeholder (ad esempio, Top Management, le Funzioni Operative, il Risk Management, le Risorse Umane, l'Ufficio Legale, la Compliance i fornitori e altri soggetti rilevanti), compresa la comunicazione sui rischi di cybersecurity esistenti ed emergenti e sulle potenziali vulnerabilità già note. Le evidenze di tali comunicazioni possono essere dimostrate con verbali di riunioni, report o e-mail.

Aspetti da valutare nel risk management

Per valutare l'applicazione dei processi di risk management agli obiettivi di cybersecurity, gli Internal Auditor possono esaminare i seguenti aspetti:

A. Come l'organizzazione valuta e gestisce il rischio di cybersecurity, incluse come le minacce e le vulnerabilità sono:
    - Inizialmente identificate e segnalate.
    - Analizzate per valutare il rischio connesso al raggiungimento degli obiettivi dell'organizzazione.
    - Mitigate, compresi i piani d'azione per ridurre il rischio a un livello accettabile.
    - Monitorate, compreso un piano di reporting continuo fino alla completa risoluzione delle minacce.

B. Come l'organizzazione ottiene aggiornamenti periodici sulla gestione del rischio di cybersecurity da parte delle funzioni aziendali, come l'Information Technology, il Risk Management, le Risorse Umane, l'Ufficio Legale, la Compliance, le Funzioni Operative, la Contabilità e la Finanza. Per ottenere informazioni si può ricorrere a un team interfunzionale di cybersecurity o a un Comitato Direttivo IT.

C. Come l'organizzazione ha assegnato le responsabilità della gestione del rischio di cybersecurity a una persona o a un team.

La persona o le persone responsabili devono comunicare periodicamente (trimestralmente, mensilmente o secondo le necessità) gli aggiornamenti sul rischio di cybersecurity all'interno dell'organizzazione e possono anche includere la necessità di risorse per l'attuazione delle strategie di mitigazione del rischio.

D. I processi di escalation dei i rischi di cybersecurity, incluse le modalità di valutazione, assegnazione e prioritizzazione del livello di minaccia o rischio. L'analisi può includere l'identificazione di:
    - Livelli di rischio definiti dall'organizzazione, come alto, moderato e basso, con spiegazioni dettagliate di ciascun livello di rischio e procedure di escalation per ogni evento di rischio.
    - Elenco dei rischi di cybersecurity attualmente identificati e le modalità di gestione di ciascun evento di rischio.
    - Requisiti legali, normativi e di compliance applicabili.
    - Impatto finanziario e non finanziario (ad esempio reputazionali) dei rischi.

E. Il processo di comunicazione dei rischi di cybersecurity al management e ai dipendenti, che comprende:
    - Formazione periodica (almeno annuale) dei dipendenti sulla cybersecurity, inclusa l'organizzazione di campagne simulate di phishing non annunciate per testare e monitorare la consapevolezza all'interno dell'organizzazione.

- Aggiornamenti sulla risoluzione dei problemi legati alla cybersecurity esistenti, con le tempistiche previste per l'implementazione dei piani d'azione.
- Monitoraggio delle non conformità inclusi gli aggiornamenti al Board e al Top Management.
- Rivalutazione delle minacce quando il risk appetite la risk tollerance dell'organizzazione subiscono modifiche.

F. I processi che l'organizzazione ha implementato per la gestione degli incidenti di cybersecurity e il ripristino delle operazioni, che includono:

- Un piano formalizzato che viene rivisto e aggiornato man mano che le operazioni dell'organizzazione cambiano nel tempo. Il piano dovrebbe comprendere:
  - Come vengono rilevati e segnalati gli incidenti.
  - Come contenere gli incidenti per evitare ulteriori danni.
  - Come l'organizzazione gestirà il ripristino e la risposta per riprendere le operazioni.
  - Come verrà analizzato l'incidente per identificare spunti di miglioramento e come prevenire eventi simili in futuro.
- Test (tabletop exercise) periodici (almeno annuali) e comunicazione dei risultati al Top Management e agli stakeholder principali. Da tali test possono emergere dei piani d'azione.

Aspetti da valutare nei processi di controllo

Per valutare l'applicazione dei processi di controllo agli obiettivi di cybersecurity, gli Internal Auditor possono esaminare i seguenti aspetti:

A. L'approccio del management per la creazione di un ambiente di controllo interno efficace per la cybersecurity, tra cui:

- Valutare e implementare i controlli necessari per mitigare i rischi elevati e proteggere i dati sensibili, critici, personali o confidenziali, sulla base del processo di risk assessment dell'organizzazione.
- Determinare le risorse necessarie per garantire il mantenimento dei controlli chiave sulla cybersecurity.
- Valutare se le verifiche sui fornitori, come parte del sistema dei controlli, include l'esame dei rapporti SOC (service organization controls) dei fornitori prima dell'inizio del rapporto commerciale e per tutta la durata del rapporto stesso.
- Verifica periodica che i controlli di cybersecurity siano efficaci nel ridurre i rischi e nel supportare il raggiungimento degli obiettivi di cybersecurity.

- Processo per la risoluzione delle carenze del sistema di controllo interno o per la gestione dei rilievi emersi dalle valutazioni effettuate dalla funzione Internal Audit o da altri fornitori di assurance (ad esempio, penetration test).

B. Il processo di sviluppo e aggiornamento delle competeze in ambito cybersecurity, comprese le modalità con cui l'organizzazione identifica le opportunità per potenziare le competenze professionali e per aumentare la cosapevolezza dell'organizzazione rispetto alle minacce emergenti.
    - Tra gli esempi vi sono la partecipazione a corsi di formazione, il coinvolgimento in gruppi di knowledge-sharing e la formazione professionale continua che comprende il conseguimento di certificazioni relative alla cybersecurity.

C. Il processo per l'identificazione, la prioritizzazione, il monitoraggio e la segnalazione delle minacce e delle vulnerabilità emergenti in materia cybersecurity svolto in maniera continuativa e sulle attività operative quotidiane. L'analisi può includere la definizione di processi per valutare le minacce e le vulnerabilità legate a tecnologie nuove o emergenti, come l'uso dell'intelligenza artificiale.

D. Processi e controlli implementati dal management per la gestione e la protezione degli asset IT durante l'intero ciclo di vita, incluso la selezione, l'utilizzo, la manutenzione e la dismissione di hardware, software e servizi forniti da terze parti. L'hardware comprende server, apparecchiature di rete (come ad esempio router o firewall), desktop, laptop, telefoni cellulari, tablet e periferiche. Il software comprende sistemi operativi (come ad esempio Windows), software di gestione aziendale (ERP – enterprise resources planning software), applicazioni, programmi antivirus e altri strumenti. Gli aspetti da valutare sull'hardware e sul software possono includere:
    - L'utilizzo da parte dell'organizzazione di crittografia, software antivirus, gestione dei dispositivi mobili, requisiti per password complesse, Virtual Private Network (VPN) e Zero Trust Networking (ZTN) per l'autenticazione oltre all'aggiornamento periodico del firmware.
    - Un processo di gestione degli asset che garantisce che l'hardware aziendale sia configurato con adeguati standard di sicurezza al momento della distribuzione e che venga correttamente smaltito al termine del suo ciclo di vita.
    - Controlli relativi ai database che includono: la limitazione degli accessi per utenti e amministratori, l'utilizzo della crittografia per la protezione dei dati, il backup e i test dei database per garantirne l'integrità e la disponibilità, l'implementazione di robusti controlli di sicurezza della rete.
    - Come vengono considerate le minacce o le vulnerabilità della cybersecurity nel ciclo di vita dello sviluppo del sistema (SDLC).
    - L'approccio che integra sviluppo, sicurezza e operazioni (DevSecOps) per garantire che il processo di sviluppo del software includa la cybersecurity e permetta l'identificazione proattiva delle vulnerabilità.

E. Processi utilizzati per rafforzare la cybersecurity, tra cui:
    - Configurazione delle impostazioni di sicurezza per ridurre al minimo il rischio di cybersecurity.
    - La gestione dei dispositivi mobili (compreso l'utilizzo della posta elettronica e delle applicazioni) è configurata per ridurre i rischi di cybersecurity e consentire la gestione da remoto in caso di compromissione del dispositivo dell'utente.
    - L'utilizzo della crittografia per proteggere i dati "at rest", come le informazioni archiviate su un hard disk, o per i dati "in transito", come la crittografia delle e-mail.
    - Patching di server o software (ad esempio un sistema operativo) con le ultime release di sicurezza.
    - Gestione dell'accesso degli utenti, come l'utilizzo dell'autenticazione a più fattori (MFA) e di ID utente unici con password complesse che scadono periodicamente.
    - Controlli di monitoraggio in atto per determinare se la disponibilità e l'utilizzo delle risorse funzionano in modo adeguato, consentendo l'esame e l'analisi di potenziali problemi di cybersecurity che minacciano le prestazioni.
    - Integrazione della cybersecurity nell'SDLC per identificare e risolvere le vulnerabilità prima che il software venga messo in produzione.

F. Controlli relativi alla rete per proteggere il perimentro di sicurezza dell'organizzazione, incluse le modalità adottare per:
    - Segmentazione della rete.
    - Firewall.
    - Controlli sugli accessi degli utenti.
    - Limitazioni alle connessioni esterne e interne.
    - Controlli relativi all’Internet of Things (IoT) per le reti interconnesse.
    - Sistemi di rilevamento/prevenzione delle intrusioni per prevenire, rilevare e recuperare gli attacchi di cybersecurity.

G. Controlli di sicurezza relativi alla comunicazione degli endpoint, applicabili a servizi come e-mail, browser Internet, videoconferenze, messaggistica (Zoom, MS Teams e altri), social media, cloud e protocolli di condivisione file. I controlli possono includere le restrizione sull'uso di determinate estensioni di file (ad esempio i file .exe) e l'autenticazione multifattore per la condivisione dei file.

Appendice A. Esempi di applicazione pratica

I seguenti esempi illustrano scenari in cui il Requisito Tematico sulla cybersecurity è applicabile

Esempio 1: la cybersecurity identificata in un incarico di Internal Audit incluso nel piano di Audit.

Quando la funzione Internal Audit completa il processo di pianificazione risk-based e include uno o più incarichi sulla cybersecurity nel piano di Audit, il Requisito Tematico è obbligatorio per la conduzione di tali incarichi. La conformità può essere garantita includendo i requisiti in uno o più incarichi previsti nel piano di Audit

La cybersecurity è un argomento ampio e non tutti i requisiti del Requisito Tematico sono applicabili a tutti gli incarichi. Quando gli Internal Auditor, sulla base del giudizio professionale, stabiliscono che uno o più requisiti del Requisito Tematico sulla cybersecurity non sono applicabili e devono essere esclusi da un incarico, devono documentare e conservare la motivazione dell'esclusione. Ad esempio, un incarico potrebbe escludere alcuni requisiti perché: la funzione Internal Audit esegue vari incarichi di cybersecurity a rotazione o ha stabilito che la rilevanza del rischio nell'incarico di Internal Audit è bassa.

Esempio 2: identificazione dei rischi di cybersecurity durante un incarico di Internal Audit non specifico sulla cybersecurity.

Gli Internal Auditor possono individuare rischi di cybersecurity anche durante la verifica di processi non direttamente legati a quest'area di rischio. Ad esempio, durante un incarico di Internal Audit sulla contabilità fornitori, gli Internal Auditor non identificano inizialmente i rischi di cybersecurity tra gli ambiti di verifica. Tuttavia, nel corso del walkthrough iniziale, gli Internal Auditor stabiliscono che tali rischi dovrebbero rientrare nell'ambito; ad esempio, emergono i rischi di cybersecurity relativi all'invio via web delle richieste iniziale di ordine di acquisto (Standard 13.2 Risk assessment dell'incarico).

Una volta identificati i rischi rilevanti, gli Internal Auditor devono esaminare il Requisito Tematico di cybersecurity e determinare quali requisiti siano applicabili. In questo esempio, si potrebbero escludere il processo di governance o il processo di risk management. Gli Internal Auditor devono documentare nelle carte di lavoro dell'incarico la motivazione dell'esclusione degli altri requisiti del Requisito Tematico sulla cybersecurity e conservare la documentazione a supporto.

Esempio 3: richiesta di un incarico di cybersecurity non incluso nel piano di Audit.

Gli stakeholder, come il Board, il management o un regulator, possono chiedere agli Internal Auditor di svolgere un incarico di cybersecurity al di fuori del piano di Audit originale. Ad esempio, se un'organizzazione subisce un attacco informatico, il Board può richiedere di svolgere un incarico di Internal Audit per valutare i controlli di cybersecurity. Il Requisito Tematico è applicabile, i requisiti devono essere valutati e le eventuali esclusioni devono essere documentate.

Appendice B. Framework di riferimento

L'organizzazione potrebbe avere proprie iniziative in ambito cybersecurity, basandosi su framework di risk management e di governance come COBIT o NIST. Gli Internal Auditor potrebbero aver già sviluppato programmi di lavoro e procedure di testing in linea con questi framework. Gli Internal Auditor dovrebbero allineare i test previsti sui controlli di cybersecurity con il Requisito Tematico per garantire una copertura adeguata. La tabella seguente mette in relazione il Requisito Tematico sulla cybersecurity con tre framework comunemente utilizzati: NIST Cybersecurity Framework 2.0, COBIT 2019 e NIST 800-53. Questi framework sono stati selezionati poiché facilmente accessibili a costo zero.

Requisiti sulla governance	**Riferimenti ai framework**		
	NIST CSF 2.0	**NIST 800-53**	**COBIT 2019**
A. Piano strategico e obiettivi di cybersecurity formalizzati e periodicamente rivisti. Gli aggiornamenti sul raggiungimento degli obiettivi di cybersecurity sono periodicamente trasmessi e rivisti dal Board, comprese le risorse e le esigenze di budget per supportare la strategia di cybersecurity.	GV.RM-01; GV.RM-02; GV.RM-03; GV.RM-04; GV.OC-02; GV.RR-03; GV.RR-04; GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-03	PM-1, PM-4; AT-2; AT-3; PM-9; PM-28	EDM01; EDM03; EDM04; APO06; APO01; APO10; APO12
B. Policy e procedure relative alla cybersecurity sono definite, aggiornate periodicamente e contribuiscono a rafforzare l'ambiente di controllo.	GV.PO-01; GV.PO-02; GV.OV-01; GV.OV-02; GV.OV-03; GV.SC-01; GV.SC-03; GV.RR-03	AC-1, PM-9; AC-1; AT-1; CA-1; CM-1; IA-1; IR-1; MP-1; PE-1	EDM01; EDM02; EDM03; APO01; APO11
C. Ruoli e responsabilità finalizzati al raggiungimento degli obiettivi di cybersecurity e presenza di un processo per valutare periodicamente le conoscenze, le competenze e le capacità del personale che ricopre ruoli in ambito cybersecurity.	GV.RR-02; GV.RR-04; GV.SC-02; GV.OC-02	PM-13; AT-2; AT-3	EDM02; APO01; APO07

D. Coinvolgimento dei principali stakeholder per discutere e intervenire sulle vulnerabilità esistenti e sulle minacce emergenti in ambito cybersecurity. Tra gli stakeholder il Top Management, le Funzioni Operative, il Risk Management, le Risorse Umane, l'Ufficio Legale, la Compliance, e altri soggetti rilevanti.	GV.OC-02; GV.RM-01; GV.RM-05; GV.RM-07; GV.OV-03; GV.SC-03	AC-1; CM-1	EDM05; EDM01.01; EDM03; MEA01.02; APO01; APO08; APO11; APO13; MEA02
Requisiti nel risk management	**NIST CSF 2.0**	**NIST 800-53**	**COBIT 2019**
A. I processi di risk assessment e risk management dell'organizzazione includono l'identificazione, l'analisi, la mitigazione e il monitoraggio delle minacce alla cybersecurity e il loro impatto sul raggiungimento degli obiettivi strategici.	GV.RM-01; GV.RM-03; GV.OC-01	AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
B. Il risk management in ambito cybersecurity riguarda tutta l'organizzazione e può includere le seguenti aree: l'information technology, il risk managment, le risorse umane, l'ufficio legale, la compliance, le funzioni operative, la supply chain, la contabilità e la finanza e altre aree.	GV.RM-01; GV.RM-05; GV.RR-01; GV.RR-02; GV.OC-03; GV.SC-07	PM-29; AT-1; PM-9; PM-28	EDM03; APO01; APO10; APO12
C. Sono state stabilite le responsabilità per la gestione del rischio di cybersecurity ed è stata identificata una persona o un team che monitora e riferisce periodicamente le modalità di gestione dei rischi di cybersecurity, e informa in merito alle risorse necessarie per mitigare il rischio e identificare le minacce emergenti in ambito cybersecurity.	GV.RR-01; GV.RR-02; GV.RR-03; GV.0V-01; GV.OV-02; GV.OV-03	PM-9; PM-29	EDM03; APO01; APO10; APO12

D. È stato stabilito un processo di escalation per segnalare tempestivamente ogni evento di rischio (emergente o già identificato) che raggiunga un livello inaccettabile, in conformità con le linee guida di risk management dell'organizzazione o per rispettare i requisiti legali e normativi applicabili. Devono essere considerati sia gli impatti finanziari che non finanziari derivanti dal rischio di cybersecurity.	GV.RM; ID.RA; RS.MA-04	CA-7; RA-3; RA-7	EDM03; APO01, APO10; APO12
E. È stato stabilito un processo per sensibilizzare il management e i dipendenti sui rischi di cybersecurity nonché per garantire una revisione periodica da parte del management di problematiche, lacune, carenze o malfunzionamenti dei controlli con procedure di reporting e piano di mitigazione.	PR.AT; GV.RR.01; GV.RR-04; GV.PO	AT-2	APO01; APO02; EDM03; MEA03
F. L'organizzazione ha implementato un processo per la gestione degli incidenti di cybersecurity e per il ripristino delle operazioni che comprende il rilevamento, il contenimento, il ripristino e l'analisi post-incidente. Tale processo viene testato periodicamente.	RS; RC	IR-4; IR-5; IR-6; IR-7; IR-8; IR-10; SA-15	DSS02; DSS03; DSS04; DSS05.07

Requisiti nei processi di controllo	NIST CSF 2.0	NIST 800-53	COBIT 2019
A. È stato stabilito un processo che garantisce l'esistenza di controlli interni e di controlli sui fornitori per proteggere la riservatezza, l'integrità e la disponibilità dei sistemi informativi e dei dati dell'organizzazione. L'adeguatezza dei controlli è valutata periodicamente per determinare il loro funzionamento in modo da promuovere il raggiungimento degli obiettivi di cybersecurity dell'organizzazione e la risoluzione tempestiva dei problemi.	ID.IM-01; ID.IM-02; ID.IM-03; PR; DE; RS; RC; ID.RA06; GV.RM-05; GV.SC; ID.IM-02; RS.MA-01; DE.CM-06	AC-3; AC-4; AC-10; AC-13; AC-17; PM-30; RA-3; SA-9; SR-2	MEA02; MEA04; EDM03; APO09; APO10; DSS01
B. È stato istituito un processo di sviluppo e aggiornamento delle competenze in ambito cybersecurity. Il processo viene rivisto periodicamente.	PR.AT-01; PR.AT-02; GV.RR-03	AT-2; AT-3; IR-2; PM-14	APOO7; DSS04
C. È stato istituito un processo per monitorare e segnalare in maniera continuativa le minacce e le vulnerabilità emergenti in materia di cybersecurity e per identificare, prioritizzare e implementare le opportunità di miglioramento nelle attività operative di cybersecurity.	ID.RA-02; ID.RA-03, ID.RA-04	CA-7; PM-31; RA-5	DSS03.05
D. La cybersecurity è inclusa nella gestione del ciclo di vita (selezione, utilizzo, manutenzione e dismissione) di tutti gli asset IT, compresi hardware, software e servizi forniti da terze parti.	ID.AM; PR.PS-03; PR.IR; DE.CM-09; ID.AM-08; ID.RA-09; PR.PS-06	AU-9; CM-7; SC-49; SC-51; CM-2; SA-3; SA-10; SA-15; SA-17; SA-20; AU-6; IR-7	DSS05.03; BAI03; BAI09; BAI03; BAI11; DSS05.01; DSS02; DSS03; DSS06.06

E. Vengono stabiliti processi per rafforzare la cybersecurity, tra cui la configurazione, la gestione dei dispositivi dell'utente finale, la crittografia, il patching, la gestione dell'accesso degli utenti e il monitoraggio della disponibilità delle risorse e della performance. Gli aspetti da valutare sulla cybersecurity sono inclusi nello sviluppo del software (DevSecOps).	PR.PS-01; PR.PS-06; PR.DS-01; PR.DS-02; PR.PS-05; DE.CM-03	CM-6; SI-2; AC-3; CA-7; SA-4; AC-16; AC-18	BAI10; DSS05; DSS06.03; DSS01.03; MEA01
F. Vengono stabiliti controlli relativi alla rete, come i controlli e la segmentazione dell'accesso alla rete, l'uso e il posizionamento dei firewall, le connessioni limitate da e verso le reti esterne, la Virtual Private Network (VPN) e Zero Trust Networking (ZTNA), i controlli dell'Internet of Things (IoT) e i sistemi di intrusion detection / prevention (IDS e IPS).	PR.IR; DE.CM-01	AC-6; AC-17; AC-18; AC-20; SC-7; SC-10; CA-8	DSS05.02
G. Vengono stabiliti controlli di sicurezza sulle comunicazioni degli endpoint per quanto riguarda servizi quali e-mail, browser Internet, videoconferenze, messaggistica, social media, cloud e protocolli di condivisione dei file.	PR.DS-01; PR.DS-02; PR.DS-10; PR.IR	AC-2; AC-16; AU-10; CA-3; SI-8; SI-20; SC-8	BAI10

Appendice C. Strumento di documentazione opzionale

Gli Internal Auditor devono esercitare il giudizio professionale per determinare l'applicabilità dei requisiti sulla base del risk assessment e documentare in modo appropriato l'esclusione di determinati requisiti. Il Requisito Tematico può essere documentato nel piano di Audit o nelle carte di lavoro dell'incarico, a seconda del giudizio professionale dell'Internal Auditor. Uno o più incarichi di Internal Audit possono coprire i requisiti ma non tutti potrebbero essere applicabili. La tabella riportata di seguito offre un'opzione per documentare la conformità al Requisito Tematico sulla cybersecurity, ma il suo utilizzo non è obbligatorio.

Cybersecurity - Governance

Requisiti	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
A. Piano strategico e obiettivi di cybersecurity formalizzati e periodicamente rivisti. Gli aggiornamenti sul raggiungimento degli obiettivi di cybersecurity sono periodicamente trasmessi e rivisti dal Board, comprese le risorse e le esigenze di budget per supportare la strategia di cybersecurity.		
B. Policy e procedure relative alla cybersecurity sono definite, aggiornate periodicamente e contribuiscono a rafforzare l'ambiente di controllo.		
C. Ruoli e responsabilità finalizzati al raggiungimento degli obiettivi di cybersecurity e presenza di un processo per valutare periodicamente le conoscenze, le competenze e le capacità del personale che ricopre ruoli in ambito cybersecurity.		

Requisiti	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
D. Coinvolgimento degli stakeholder rilevanti per discutere e intervenire sulle vulnerabilità esistenti e sulle minacce emergenti in ambito cybersecurity. Tra gli stakeholder il Top Management, le Funzioni Operative, il Risk Management, le Risorse Umane, l'Ufficio Legale, la Compliance, e altri soggetti rilevanti.		

Cybersecurity - Risk Management

Requisiti	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
A. I processi di risk assessment e risk management dell'organizzazione includono l'identificazione, l'analisi, la mitigazione e il monitoraggio delle minacce alla cybersecurity e il loro impatto sul raggiungimento degli obiettivi strategici.		
B. Il risk management in ambito cybersecurity riguarda tutta l'organizzazione e può includere le seguenti aree: l'information technology, l'enterprise risk management, le risorse umane, l'ufficio legale, la compliance, le foperations, la supply chain, la contabilità e la finanza e altre aree.		

Requisiti	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
C. Sono state stabilite le responsabilità per la gestione del rischio di cybersecurity ed è stata identificata una persona o un team che monitora e riferisce periodicamente le modalità di gestione dei rischi di cybersecurity, e informa in merito alle risorse necessarie per mitigare il rischio e identificare le minacce emergenti in ambito cybersecurity.		
D. È stato stabilito un processo di escalation per segnalare tempestivamente ogni evento dirischio (emergente o già identificato) che raggiunga un livello inaccettabile, in conformità con le linee guida di risk management dell'organizzazione o per rispettare i requisiti legali e normativi applicabili. Devono essere considerati sia gli impatti finanziari che non finanziari derivanti dal rischio di cybersecurity.		
E. È stato stabilito un processo per sensibilizzare il management e i dipendenti sui rischi di cybersecurity nonché per garantire una revisione periodica da parte del management di problematiche, lacune, carenze o malfunzionamenti dei controlli con procedure di reporting e remediation.		
F. L'organizzazione ha implementato un processo per la gestione degli incidenti di cybersecurity e per il ripristino delle operazioni che comprende il rilevamento, il contenimento, il ripristino e l'analisi post-incidente. Tale processo viene testato periodicamente.		

Cybersecurity - Processi di controllo

Requisiti	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
A. È stato stabilito un processo che garantisce l'esistenza di controlli interni e di controlli sui fornitori per proteggere la riservatezza, l'integrità e la disponibilità dei sistemi informativi e dei dati dell'organizzazione. L'adeguatezza dei controlli è valutata periodicamente per determinare il loro funzionamento in modo da promuovere il raggiungimento degli obiettivi di cybersecurity dell'organizzazione e la risoluzione tempestiva dei problemi.		
B. È stato istituito un processo di sviluppo e aggiornamento delle competenze in ambito cybersecurity. Il processo viene rivisto periodicamente.		
C. È stato istituito un processo per monitorare e segnalare in maniera continuativa le minacce e le vulnerabilità emergenti in materia di cybersecurity e per identificare, prioritizzare e implementare le opportunità di miglioramento nelle attività operative di cybersecurity.		
D. La cybersecurity è inclusa nella gestione del ciclo di vita (selezione, utilizzo, manutenzione e dismissione) di tutti gli asset IT, compresi hardware, software e servizi forniti da terze parti.		

Requisiti	Applicabilità del requisito o giustificazione per l'esclusione	Documentazione di riferimento
E. Vengono stabiliti processi per rafforzare la cybersecurity, tra cui la configurazione, la gestione dei dispositivi dell'utente finale, la crittografia, il patching, la gestione dell'accesso degli utenti e il monitoraggio della disponibilità delle risorse e delle performance. Gli aspetti da valutare sulla cybersecurity sono inclusi nello sviluppo del software (DevSecOps).		
F. Vengono stabiliti controlli relativi alla rete, come i controlli e la segmentazione dell'accesso alla rete, l'uso e il posizionamento dei firewall, le connessioni limitate da e verso le reti esterne, la Virtual Private Network (VPN) e Zero Trust Networking (ZTNA), i controlli dell'Internet of Things (IoT) e i sistemi di intrusion detection/prevention (IDS e IPS).		
G. Vengono stabiliti controlli di sicurezza sulle comunicazioni degli endpoint per quanto riguarda servizi quali e-mail, browser Internet, videoconferenze, messaggistica, social media, cloud e protocolli di condivisione dei 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 www.theiia.org.

Esclusione di responsabilità

Copyright

Febbraio 2025

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101