Requisiti Tematici – Consigli pratici di applicazione e appunti tratti dalla valutazione esterna della qualità

Management Summary

Con l'introduzione dei Global Internal Audit Standards 2024 (di seguito denominati "Standard"), The Institute of Internal Auditors (IIA) ha creato un nuovo elemento obbligatorio nell'ambito dell' "International Professional Practices Framework" (IPPF): i "Requisiti Tematici" (Topical Requirements - TR). Questi definiscono un ambito minimo vincolante per gli audit in determinate aree di rischio e mirano a garantire standard di qualità uniformi per l'audit interno a livello mondiale.

Nel 2026 entreranno in vigore i primi TR, che richiederanno ai revisori interni di allineare di conseguenza i propri processi di pianificazione e audit. L'IIA fornisce diversi documenti ufficiali che chiariscono le questioni chiave e supportano l'attuazione pratica. Un punto chiave nell'implementazione è che i TR devono essere utilizzati solo se un tema è classificato come materiale nel contesto dell'analisi periodica generale dei rischi (o durante l'analisi dei rischi a livello di engagement) e se, per tale tema, è previsto un verifica dell'assurance. Questa materialità viene valutata nel contesto della propensione al rischio e degli obiettivi strategici dell'organizzazione. La questione se un TR debba essere applicato dipende dal risultato dell'analisi dei rischi e dall'ambito dell'audit che ne deriva e richiede il giudizio professionale del revisore interno.

L'IIA sottolinea esplicitamente l'importanza di un processo di giustificazione comprensibile. Se un TR non viene applicato o solo parzialmente, anche se è stato identificato un rischio materiale nell'ambito di applicazione di un TR, deve essere documentato perché il rispettivo TR o requisito non è rilevante o non corrisponde alla causa del rischio.

Considerando questi aspetti, il gruppo di lavoro Professional Services Firms dell'IIA Switzerland ha elaborato il presente white paper. Il documento combina i risultati dei primi progetti pilota di applicazione nel mercato svizzero con prospettive provenienti da valutazioni esterne della qualità. L'obiettivo è supportare i responsabili di audit nell'implementazione coerente, orientata al rischio e pragmatica dei nuovi requisiti. Il documento non pretende di essere completo né ufficialmente vincolante e rappresenta esclusivamente l'opinione e l'interpretazione del team di autori e del gruppo di lavoro al momento della sua pubblicazione; è pensato come guida pratica.

Introduzione – Orientamento sui TR e fonti ufficiali

L'IIA fornisce tutte le informazioni essenziali sui TR in modo centralizzato sul proprio sito web.

- Link alla pagina: https://www.theiia.org/en/standards/2024-standards/topical-requirements/

Questo contenuto viene aggiornato costantemente e costituisce la base decisiva per l'applicazione dei TR nell'attività quotidiana di audit. Sono inclusi i TR pubblicati, le consultazioni in corso e le pubblicazioni future. Per ogni TR viene chiaramente indicato quando diventa obbligatorio — di norma un anno dopo la pubblicazione.

I primi TR entreranno in vigore come segue:

- Cybersecurity: dal 5 febbraio 2026
- Terze parti: dal 15 settembre 2026
- Comportamento organizzativo: dal 15 dicembre 2026
- Resilienza organizzativa: dal 30 aprile 2027

Oltre al TR stesso, l'IIA fornisce diversi materiali complementari che supportano un'applicazione coerente:

- La **Guida all'applicazione dei requisiti tematici**, disponibile in più lingue, che fornisce indicazioni generali e pratiche per l'applicazione.
  - https://www.theiia.org/en/content/topical-requirements/topical-requirements-application-guidance
- Una **sezione FAQ** sul sito dei TR.
- Il documento **Assessing Topical Requirements Conformance** (Insights to Quality), che fornisce indicazioni su come i TR vengono visti nel contesto delle valutazioni interne ed esterne della qualità e su come le funzioni di audit interno possano prepararsi attraverso un'implementazione significativa e una documentazione trasparente.
  - https://www.theiia.org/globalassets/site/content/insights-to-quality/insights-to-quality-assessing-topical-requirements-conformance.pdf

Per l'audit interno è consigliabile istituire un monitoraggio strutturato e regolare, al fine di tenere conto tempestivamente degli aggiornamenti. Ciò include in particolare:

- la rilevazione precoce di nuovi TR o revisioni,
- partecipazione ai processi di consultazione,
- garantire un'attuazione tempestiva.

Prospettive sugli argomenti previsti

L'IIA ha ulteriori TR in preparazione. Al momento della pubblicazione del presente documento è in corso il processo di consultazione per il TR "Anti-corruzione". Inoltre, è stata annunciata una Research Letter sul tema "Talent Management", per la quale il processo di consultazione è previsto per ottobre 2026. Questi due TR non saranno applicabili prima del 2027.

Inoltre, l'IIA presenta regolarmente il proprio Risk and Topic Radar in eventi e webinar. Gli argomenti che si trovano nello stato "Mature" nel grafico sottostante (vedi Fig. 1, in blu) sono considerati consolidati; in questi casi i TR sono particolarmente probabili. Inoltre, tra gli altri, sono in fase di valutazione

Argomenti importanti e caratterizzati da un'elevata dinamicità, che appaiono nel radar come "Emerging" (vedi Fig. 1, in verde), attualmente non sono tradotti in TR.

Il processo di monitoraggio regolare raccomandato nella sezione precedente dovrebbe quindi includere anche una revisione periodica del sito web dell'IIA per rimanere informati nelle prime fasi delle nuove consultazioni e dei futuri argomenti TR.

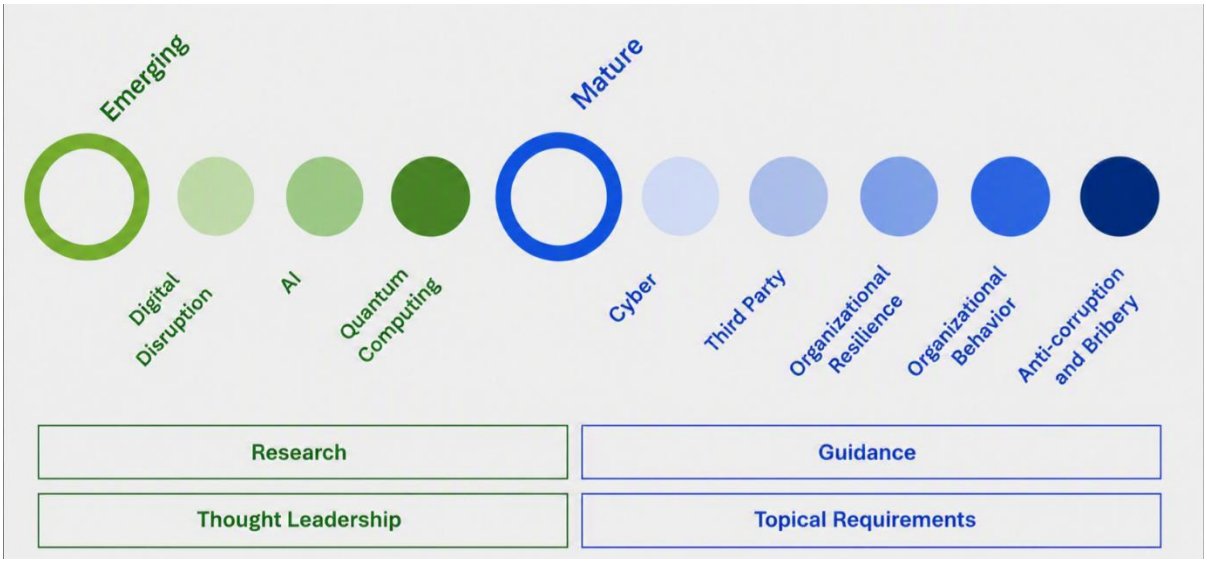

Fig. 1: "Il radar di maturità del rischio e dei temi dell'IIA", fonte: IIA

Applicazione dei TR

I TR sono una componente vincolante dell'IPPF dell'IIA e sono quindi obbligatori per gli verifica dell'assurance, analogamente agli Standard. Per incarichi di consulenza in aree di rischio rilevanti, l'applicazione è raccomandata, ma non obbligatoria.

La Guida all'applicazione dei requisiti tematici specifica che un TR può essere applicato nei seguenti casi:

- se l'argomento è espressamente incluso come incarico di audit nel piano di audit,
- se l'argomento viene identificato durante un incarico di audit,
- se l'argomento è incluso in un incarico di audit, anche se non era originariamente previsto nel piano di audit.

L'identificazione degli argomenti di audit avviene di norma nell'ambito dell'analisi periodica dei rischi (in conformità allo Standard 9.4), durante l'analisi dei rischi a livello di engagement (in conformità allo Standard 13.2) o nel corso dello svolgimento dell'audit. Un TR deve essere applicato non appena un rischio corrispondente viene identificato e valutato come materiale. Di conseguenza, nell'ambito della rispettiva analisi dei rischi, occorre verificare se esistono rischi correlati ai TR vigenti. Se un tale argomento è incluso sulla base dell'analisi dei rischi, di un contributo degli stakeholder o durante l'esecuzione di un mandato di audit, deve essere applicato il corrispondente TR.

Non appena un rischio viene classificato come materiale e un TR risulta pertanto applicabile, il dipartimento di audit interno deve tenerne conto, ossia deve analizzarne e documentarne l'applicabilità. Il risultato di questa analisi può essere l'applicazione del TR nell'audit oppure la non considerazione parziale o totale di alcuni elementi del TR. Come minimo, tale valutazione deve essere garantita a livello del rispettivo incarico. Le raccomandazioni complementari dell'IIA forniscono tuttavia la base per un approccio olistico che copre l'intero ciclo di audit, dalla pianificazione periodica alla pianificazione a livello di incarico, fino allo svolgimento dell'incarico in conformità con gli Standards.[1] Ciò vale anche in caso di co-sourcing e outsourcing di un incarico, fermo restando che il committente rimane responsabile del rispetto dei requisiti applicabili lungo l'intero ciclo di vita dell'incarico.

[1] Si veda, ad esempio, l'IIA Topical Requirements – Application Guidance, capitolo 4: Applying Topical Requirements in the Audit Lifecycle.

A supporto di ciò, il gruppo di lavoro IIAS fornisce un albero decisionale che presenta sistematicamente il processo per determinarne l'applicabilità (vedi Fig. 2). Rende più facile valutare i fattori rilevanti in modo conclusivo e coerente. L'albero decisionale indica anche in quali casi è necessaria una documentazione comprensibile dell'approccio "conformarsi o spiegare" (vedi ulteriori dettagli nella sezione successiva).

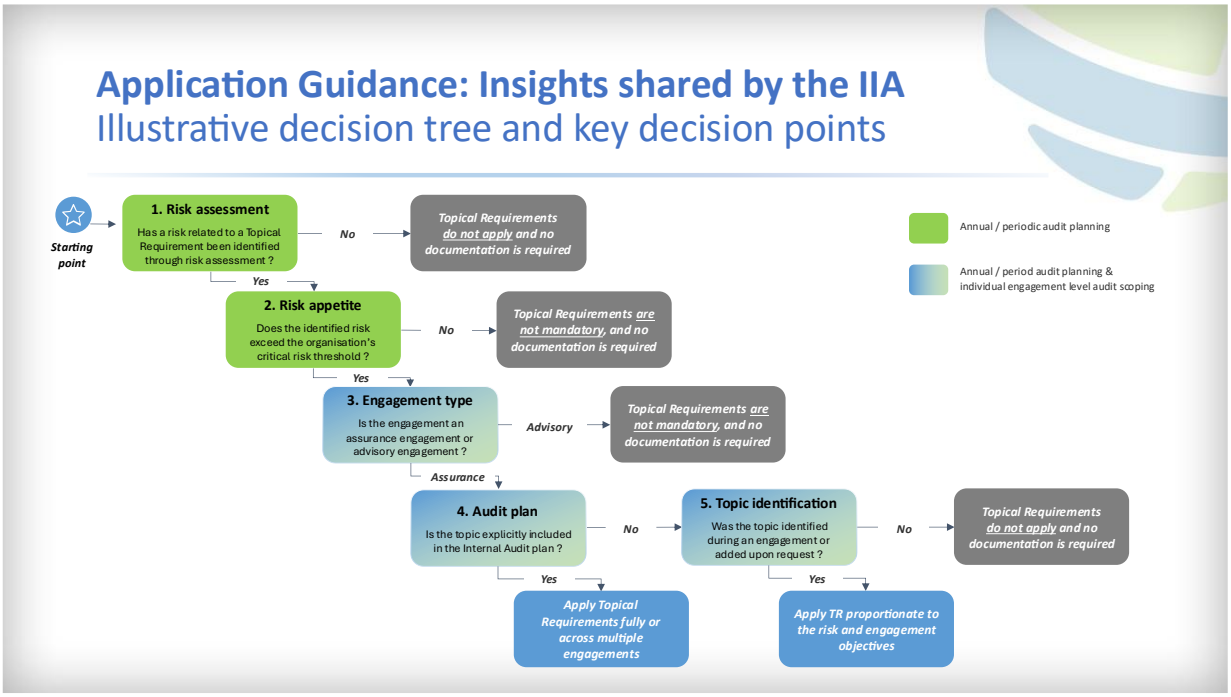

Fig. 2: Albero decisionale per l'applicazione dei Requisiti Tematici,
fonte: gruppo di lavoro IIAS "Professional Services Firms"

Giudizio professionale nell'applicazione

Il giudizio professionale è centrale in tutte le decisioni relative all'applicazione del TR. L'IIA fa esplicitamente riferimento all'approccio "conformarsi o spiegare / comply or explain" qualora un rischio materiale identificato renda obbligatoria l'applicazione di un TR e il dipartimento di audit interno, ciononostante, non lo includa nell'audit:

- Se alcuni requisiti di un TR non sono applicabili a causa della natura, del contesto o della causa di un rischio, ciò deve essere chiaramente giustificato e documentato.
- Se, ad esempio, un rischio deriva da una debolezza del controllo operativo, potrebbe essere che i requisiti specifici del controllo siano principalmente rilevanti e che alcuni elementi di governance del TR non vengano applicati.

La guida applicativa sottolinea che circostanze eccezionali, come vincoli di risorse o caratteristiche specifiche di settore, possono anche portare a deviazioni giustificate. In tali casi, il revisore dovrebbe definire misure alternative che corrispondano allo scopo del rispettivo requisito. Può essere preso in considerazione anche il lavoro di altri fornitori di assurance interne ed esterne. In questo caso è assolutamente necessaria una documentazione trasparente e comprensibile.

Copertura dei requisiti TR su diversi anni o ordini

Se un tema di audit viene esaminato nell'arco di più anni, il relativo TR deve essere preso nuovamente in considerazione per ogni incarico di audit e la sua applicabilità deve essere verificata. I requisiti possono essere distribuiti su diversi audit, anche su più anni, purché sia chiaramente documentato:

- quali elementi sono stati trattati e quando,
- quali parti sono state deliberatamente rimandate agli anni successivi,
- e perché questa decisione è tecnicamente giustificabile.

Ciò significa che non tutti i requisiti devono necessariamente essere coperti in un unico incarico di audit.

La guida applicativa richiede che tutte le decisioni discrezionali (ad esempio applicazioni parziali o casi di non applicazione) siano documentate nei documenti di pianificazione, nei working paper o nelle matrici di applicabilità e presentate in modo comprensibile durante i controlli di qualità.

Aspettative della documentazione

L'applicazione del TR, così come l'omissione parziale o totale di alcuni elementi a seguito di decisioni discrezionali tecniche, deve essere documentata in modo che una terza parte indipendente possa comprendere le decisioni. La documentazione può essere effettuata direttamente nei punti del ciclo di vita dell'audit in cui viene analizzata l'applicabilità (vedi "Albero decisionale per l'applicazione dei TR" in Fig. 2).

Per documentare l'applicazione del TR in esame, le guide utente del rispettivo TR forniscono in appendice, come supporto, uno strumento opzionale o una tabella di documentazione.

Nella valutazione, ad esempio nel contesto di una valutazione esterna della qualità (EQA), è fondamentale che le decisioni prese e le loro giustificazioni siano sufficientemente documentate e quindi comprensibili per terzi. I TR come parte integrante dell'IPPF sono incorporati nella valutazione dei rispettivi principi, specialmente nel contesto della pianificazione, conduzione e comunicazione degli esami. Non esiste una valutazione separata dei singoli TR.

Se i singoli TR sono rilevanti per determinati test, uno standard può essere classificato come "pienamente conforme" secondo un'EQA solo se tutti gli elementi dello standard sottostante sono stati soddisfatti.

Applicazione in concomitanza con i requisiti normativi

Come spiegato nella guida applicativa ufficiale dell'IIA, si applica quanto segue:

- Se le normative legali o le normative esterne impongono requisiti più severi o più ampi rispetto al TR, tali requisiti determinano l'ambito dell'audit.

In tali casi, la revisione interna deve adottare un approccio basato sul rischio e comparativo, bilanciando i requisiti normativi, il TR e altri quadri di riferimento riconosciuti.

Va sottolineato che i TR non specificano il disegno organizzativo degli argomenti oggetto di audit, bensì definiscono l'approccio di audit. Il loro scopo è garantire un approccio coerente nelle aree critiche di audit e rispettare i requisiti di qualità di base.

Reporting degli aspetti TR

La conformità ai TR deve essere documentata nell'ambito della pianificazione e dell'esecuzione dell'audit ed è monitorata anche dal Programma di assurance e miglioramento della qualità (QAIP) del dipartimento di audit interno.

Non è necessario un rapporto separato sulla conformità ai TR (ad esempio alla direzione generale e/o al consiglio d'amministrazione). Piuttosto, questi aspetti devono essere implicitamente considerati nel rapporto generale sul QAIP.

Assistenza per valutatori EQA

Per i valutatori EQA, il contenuto ufficiale dell'IIA – in particolare i materiali disponibili sul sito web – rappresenta un punto di riferimento chiave. Essi definiscono le aspettative dell'IIA per l'attuazione del TR e per la valutazione della conformità nel contesto delle ispezioni di qualità. Di particolare rilievo è il documento "Assessing Topical Requirements Conformance" (Insights to Quality), che fornisce indicazioni dettagliate sulla sua applicazione.

I TR sono una componente obbligatoria dell'IPPF e sono quindi valutati nel contesto di valutazioni interne ed esterne di qualità analoghe ad altri elementi dell'IPPF, come gli standard. Il Manuale di Valutazione della Qualità 2024 dell'IIA afferma che i valutatori dovrebbero rivedere il piano di audit basato sul rischio per assicurarsi che i TR in vigore durante il periodo di audit siano stati correttamente presi in considerazione. Questo esame viene solitamente svolto, tra le altre cose, ispezionando i working paper a livello degli esami individuali.

Il documento "Assessing Topical Requirements Conformance" chiarisce come le funzioni di audit interno e i valutatori dovrebbero procedere nella valutazione della TR Conformity. In questo contesto, l'IIA raccomanda in particolare quanto segue per gli audit interni:

- Integrazione del TR nei processi di pianificazione e test,
- Documentazione trasparente dell'applicabilità e delle giustificazioni per i casi di non applicazione,
- Garantire che i processi di audit, i documenti di lavoro e i documenti riflettano la TR Conformity in modo comprensibile.

Gli valutatori terranno quindi conto, a seconda delle modalità di attuazione dei TR nelle singole funzioni di revisione interna, dei diversi elementi del processo di audit già in sede di analisi dell'audit universe, di analisi dei rischi e di pianificazione dell'Internal Audit, valutando se siano presenti temi coperti dai TR.

I documenti autorevoli utilizzati dagli valutatori includono:

- Analisi del rischio e piano di audit (pianificazione periodica così come a livello di mandato di revisione),
- Memorandum di pianificazione e documenti di lavoro a livello di mandato di revisione,
- Matrici di controllo del rischio,
- Guida all'uso del TR, "Strumento di documentazione" o la corrispondente checklist,
- Copertura del TR nel QAIP.

Focus Cyber-TR: Panoramica delle aree da esaminare

- **Governance:** Valutazione della gestione strategica e dell'ancoraggio strutturale. Di seguito viene esaminato:
  - Esistenza di una strategia formale di cybersecurity che venga regolarmente aggiornata e sottoposta a revisione dal consiglio di amministrazione (inclusa l'approvazione del budget).
  - Stabilire linee guida chiare e definire ruoli e responsabilità all'interno dell'organizzazione.
  - Garantire e valutare le conoscenze e le competenze specialistiche necessarie dei collaboratori responsabili.
  - Gestione degli stakeholder: Coinvolgimento attivo degli stakeholder come Direzione, HR, legal, compliance e fornitori nel dialogo su minacce e vulnerabilità.
- **Gestione del rischio:** Revisione dei processi di gestione del rischio informatico. Di seguito viene esaminato:
  - Identificare, analizzare, mitigare e monitorare sistematicamente le minacce informatiche in tutte le unità organizzative.
  - Chiara assegnazione delle responsabilità per il monitoraggio e la segnalazione continua della situazione di rischio.
  - Introdurre processi per un'escalation rapida in caso di superamento della soglia, nonché misure per promuovere la consapevolezza generale del rischio.
  - Validazione di un processo di risposta e recupero (rilevamento, contenimento, follow-up) che venga regolarmente testato.
- **Processi di controllo:** verificare se sono in atto controlli interni e relativi ai fornitori per proteggere la riservatezza, l'integrità e la disponibilità di sistemi e dati. Ciò include, tra l'altro:
  - Una gestione del ciclo di vita di tutti gli asset IT (hardware, software, servizi esterni) dalla selezione alla dismissione.
  - Monitoraggio continuo delle vulnerabilità e gestione dei talenti per promuovere le competenze tecniche.
  - Processi per rafforzare la sicurezza IT, inclusi crittografia, gestione delle patch, gestione degli accessi, sviluppo software (DevSecOps) e configurazione.
  - Controlli di rete, come segmentazione di rete, firewall, accesso VPN/Zero Trust (ZTNA), controlli IoT e sistemi di rilevamento e mitigazione intrusioni (IDS/IPS).
  - Sicurezza degli endpoint per servizi come email, browser, videoconferenze e applicazioni cloud.

Organizzazione e pianificazione di un esame utilizzando l'esempio di Cyber-TR

Trigger per l'esame

In linea di principio, i requisiti TR devono essere applicati non appena il tema della cybersecurity viene identificato come rischio materiale nel contesto dell'analisi periodica dei rischi e per tale tema è previsto un verifica dell'assurance. Ciò si applica se l'argomento è espressamente incluso nel piano di audit, se si presenta come rischio materiale nel contesto di un altro incarico di audit o se gli stakeholder richiedono un ulteriore incarico di audit non pianificato.

Nella pianificazione dettagliata del mandato di audit deve essere dimostrato che i singoli requisiti del TR sono stati verificati in termini di applicabilità. Se si decide di non includere determinati elementi, o di includerli solo parzialmente, nell'ambito dell'audit, tale deviazione deve essere giustificata e documentata. La deviazione può anche essere sintetizzata, ad esempio per una delle tre aree del TR – governance, gestione del rischio, processi di controllo – se, ad esempio, gli aspetti di governance non devono far parte dell'audit pianificato per una ragione comprensibile (ad esempio perché verificati da un altro fornitore di assurance, inclusi nella pianificazione pluriennale, ecc.).

Non è obbligatorio che un singolo audit copra contemporaneamente tutti i requisiti di cybersecurity. Tuttavia, un audit mirato è consigliabile per vari motivi, poiché un audit completo è logisticamente e tecnicamente difficile da rappresentare, specialmente nel caso del Cyber-TR. Il dipartimento di audit interno può suddividere i requisiti su diversi audit e su più anni. Tuttavia, il presupposto per questa organizzazione è che sia documentato quali argomenti sono stati trattati e quando, quali aspetti sono stati deliberatamente rinviati e perché ciò sia tecnicamente giustificabile. L'applicazione dei requisiti deve inoltre essere presentata in modo trasparente e comprensibile per terzi nei documenti di pianificazione e nei working paper.

Pianificazione degli audit

Per quanto riguarda i contenuti, l'IIA è fortemente orientata verso standard consolidati in termini di contenuti. Il TR Cybersecurity cita il National Institute of Standards and Technology (NIST) fin dall'inizio per stabilire le definizioni di base di cybersecurity e sicurezza informatica. Inoltre, il TR richiede che il dipartimento di audit interno adotti un approccio comparativo, specialmente se esistono già requisiti normativi o se gli audit vengono effettuati sulla base di quadri riconosciuti a livello internazionale. Allineare la pianificazione delle ispezioni al quadro del NIST è quindi esattamente in linea con questa idea.

Esempio di piano di audit su un periodo di 3 anni secondo i requisiti minimi:

Anno	Funzione centrale del NIST	Focus secondo TR-Cybersecurity	Obiettivi specifici dell'audit e requisiti TR
Anno 1	Identify (Identificazione)	Governance & Foundation (parti della gestione e dei controlli del rischio)	Strategia e ruoli: Avere una strategia formale, definire le responsabilità e coinvolgere gli stakeholder. Identificazione del rischio: Processi per l'analisi delle minacce informatiche in tutta l'organizzazione.

			Gestione degli asset: La cybersecurity nel ciclo di vita di tutti gli asset IT (hardware, software, fornitori).
Anno 2	Protect (Proteggi)	Processi di controllo preventivo (controlli e gestione specifica del rischio)	Sicurezza di sistema e rete: Gestione degli accessi, crittografia, gestione delle patch, DevSecOps. Infrastrutture: Controlli di rete (firewall, ZTNA, segmentazione) e sicurezza degli endpoint (email, cloud, browser). Fattore umano: Gestione dei talenti per mantenere le competenze tecniche e aumentare la consapevolezza tra i dipendenti.
Anno 3	Detect, Respond, Recover (Rilevare, rispondere, recuperare)	Monitoraggio e Gestione degli Eventi (Controlli Residui e Gestione del Rischio)	Monitoraggio: Monitoraggio continuo delle vulnerabilità e uso di sistemi di rilevamento/prevenzione di intrusioni (IDS/IPS). Escalation: Processi per segnalare rapidamente rischi inaccettabili alla direzione. Gestione degli incidenti: Implementazione e test regolare di un processo di risposta agli incidenti e di recupero (rilevamento, contenimento, recupero, follow-up).

Questo white paper è stato elaborato dal gruppo di lavoro Professional Services Firms dell'IIA Switzerland. I coautori Urgent Azizi, Markus Berger, Christian Jung e Markus Pfeiler hanno raccolto e integrato i contributi e le opinioni di ulteriori esperti nonché dell'IIA Switzerland. Il presente white paper ha l'obiettivo di supportare i revisori interni nell'attuazione dei Topical Requirements e intende fungere da guida orientativa per la loro applicazione.