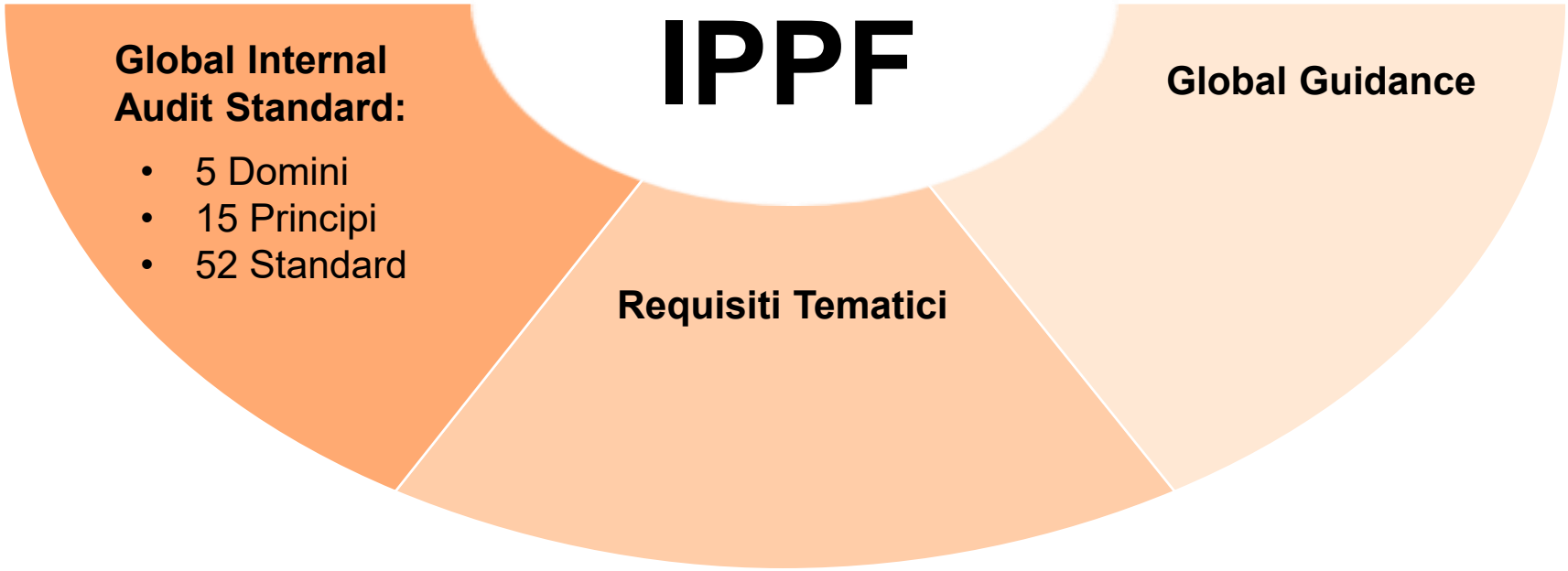
Internal Audit 2026: applicazione dei nuovi Topical Requirements sulla Digital Assurance

Agenda

1. International Professional Practices Framework (IPPF)
2. Requisito tematico sulla Cybersecurity
3. L’esperienza di Iveco
4. L’esperienza di Barilla
5. In conclusione

International Professional Practices Framework (IPPF)

L'IPPF è il quadro di riferimento globale sviluppato dall'Institute of Internal Auditors (IIA) per guidare la professione di Internal Auditing. Sistema coerente di **standard, requisiti e raccomandazioni**.



I Global Internal Audit Standard ed i **Requisiti Tematici** forniscono la **base autorevole delle pratiche di audit.**

IPPF: focus sui requisiti tematici

Requisito tematico:	**fornisce chiare indicazioni** per gli internal auditor e definisce un livello minimo di riferimento per gli audit che insistono **su determinati rischi**.
Applicabilità:	possono essere applicati **sia quando il tema è incluso nel piano di audit sia quando il tema viene identificato durante lo svolgimento di un incarico di audit** che non era originariamente previsto nel piano di audit.
Documentazione:	ogni volta che viene confermata **l'applicabilità** di un requisito dei **Topical Requirements**, questa valutazione deve essere **documentata e conservata**. Non tutti i requisiti devono essere necessariamente applicabili a ogni singolo incarico di audit, quindi, se alcuni requisiti non vengono applicati, è necessario fornire una giustificazione che deve anch'essa essere documentata e conservata.
Conformità:	la **conformità ai Topical Requirements è obbligatoria**. Durante le valutazioni di qualità, sarà esaminato se i requisiti sono stati rispettati o meno.

Requisito tematico sulla Cybersecurity

Pubblicato il 5 Febbraio 2025 ed **entrato in vigore dal 5 Febbraio 2026** (è il primo di una serie).

E' strutturato nelle sezioni Governance, Risk management e Controlli.

Fornisce una **baseline minima di criteri** per svolgere incarichi di assurance in materia di cybersecurity, garantendo **coerenza, qualità e confrontabilità** delle valutazioni svolte dalle funzioni di Internal Audit.

Il Topical Requirement cybersecurity **si applica** sia per le **verifiche specifiche sia** nel considerare il rischio in oggetto **in altre verifiche** (es: di processo, di compliance, ecc).

Agevola il dialogo tra le funzioni di controllo e le funzioni di linea.

La conformità ai Requisiti Tematici è **obbligatoria** per i servizi di **assurance** e **raccomandata** per i servizi di **advisory.**

Requisito tematico sulla Cybersecurity: governance

Gli Internal Auditor in ambito **IT / Digital audit** devono valutare i seguenti aspetti:

- **strategia di cybersecurity:** deve essere formalmente definita ed aggiornata periodicamente, deve prevedere obiettivi chiari.
- **politiche e procedure relative alla cybersecurity:** devono essere stabilite ed aggiornate periodicamente.
- **ruoli e responsabilità:** devono essere definiti i ruoli e responsabilità che supportano gli obiettivi di cybersecurity.
- **stakeholder rilevanti:** devono essere identificati e coinvolti gli **stakeholder rilevanti** (come la Direzione, il Risk Management, le risorse umane, il legale, i fornitori e altri) per **discutere e agire** riguardo alle **vulnerabilità** esistenti e alle **minacce** emergenti nell'ambiente di **cybersecurity**.

Requisito tematico sulla Cybersecurity: risk management

Gli Internal Auditor in ambito **IT / Digital audit** devono valutare i seguenti aspetti:

- I processi **di risk assessment e risk management** dell'organizzazione devono **includere il rischio cyber** e i suoi impatti.
- Il processo di **valutazione e gestione del rischio** deve includere l'identificazione, l'analisi, la mitigazione e il monitoraggio delle minacce di cybersecurity nonché il loro impatto nel raggiungimento degli obiettivi strategici.
- devono essere definite **responsabilità** e **accountability** per la gestione del rischio di cybersecurity.
- deve esistere un processo rapido di **escalation** per qualsiasi rischio di cybersecurity (emergente o precedentemente identificato) che raggiunga un livello inaccettabile.
- deve esistere un processo per **trasmettere la consapevolezza del rischio di cybersecurity** a management e dipendenti.
- Deve essere implementato un processo di **risposta e recupero da incidenti di cybersecurity.**

Requisito tematico sulla Cybersecurity: controlli

Gli Internal Auditor in ambito **IT / Digital audit** devono valutare i seguenti aspetti:

- Deve essere stabilito un processo per garantire che siano posti in essere sia i **controlli interni** sia i **controlli presso i fornitori,** per proteggere la riservatezza, integrità e accessibilità dei sistemi e dei dati.
- Deve essere stabilito un processo di **gestione delle risorse umane** che includa **formazione** per **sviluppare** e **mantenere** le competenze tecniche necessarie per le operazioni di cybersecurity.
- Deve essere stabilito un processo per **monitorare continuamente** e **segnalare** le minacce e le vulnerabilità emergenti in ambito cybersecurity.
- La **cybersecurity** deve essere considerata nel **ciclo di vita** di tutti gli **asset IT.**
- Sono definiti **processi per rafforzare la cybersecurity** (controllo accessi, crittografia, patching, ecc).
- Devono essere stabiliti **controlli legati alla rete** (VPN, IPS, IDS, ecc).
- Devono essere stabiliti **controlli di sicurezza per la comunicazione agli endpoint.**

L’esperienza di IVECO

Alessandra Ramorino

Ramorino, Chief Risk and Internal Audit Officer | Iveco Group

L’esperienza di IVECO

Elisabetta Grignani

Head of IT Audit and Digital Transformation | Iveco Group

Daniele Rusconi

Associate IT Audit Director | Barilla

L’esperienza di Barilla

In conclusione: la #digitalassurance non è piu una scelta

- Gli **IPPF** (International Professional Practices Framework: Global Internal Audit Standard e Requisiti tematici) forniscono la **base autorevole a cui la professione si ispira.**
- La conformità ai Requisiti Tematici è **obbligatoria** per i servizi di **assurance** e **raccomandata** per i servizi di **advisory**
- Il **requisito tematico sulla cybersecurity** attribuisce un **ruolo** anche alla funzione di **IT/Digital Audit** nel presidio del sistema di gestione del rischio e di controllo interno.
- Il requisito tematico **cybersecurity** deve anche essere **valutato** nel contesto di **altre verifiche** (es: di processo, di compliance, ecc).
- Il requisito **richiede** alla funzione di **Internal Audit** ed **IT/Digital Audit** di dotarsi di **competenze "nuove e specialistiche"** che necessitano di percorsi di **upskilling/digital skilling continui.**

Grazie!

Dino Ponghetti,

Partner, OTS | PwC Italia
dino.ponghetti@pwc.com

CISA, CGEIT, Lead Audit ISO20000,
ISO22031, ISO27001, DPO

Giuseppe Garzillo

Partner, OTS | PwC Italia
giuseppe.garzillo@pwc.com

Certified internal auditor