Cyber resilienza e assurance: approcci per Internal Audit funzioni di controllo

Convegno Nazionale AIIA

Giugno 2026

Wolters Kluwer

TeamMate®

Il webinar sta per iniziare

Domande sui contenuti in qualsiasi momento

Assistenza per eventuali problemi tecnici

Scarichi il PDF delle diapositive nella sezione Lista Risorse

Per ottenere i CPE è necessario soddisfare tutti i requisiti elencati nel grafico «Certificazione».

Il certificato CPE può essere scaricato immediatamente una volta soddisfatti i requisiti

Il webinar sarà disponibile per la visione on-demand circa 24 ore dopo l'evento

Agenda

- Trend e Framework in ambito cyber
- Come abilitare audit cyber più efficaci e strutturati e in collaborazione tra funzioni di controllo
- Approccio Pratico di come la tecnologia può contribuire a migliorare le attività di audit e controllo (Demo)
- Q&A

Gianluca Saccone

Gianluca, Senior Sales Manager di Wolters Kluwer TeamMate per Italia e Malta, ha 9 anni di esperienza in ambito commerciale ed è laureato in Giurisprudenza presso l'Universitá degli Studi Roma Tre.

Prima di ricoprire questo ruolo in Internal audit, risk management e compliance, ha collaborato con le principali istituzioni finanziarie italiane ed europee supportandole nella gestione di rischi finanziari, compliance e analisi dei dati.

Gianluca Saccone
Sales Manager
Wolters Kluwer TeamMate
gianluca.saccone@wolterskluwer.com

Vanessa Olarte Bendezu, CIA, CFE

Vanessa è Business Solutions Manager in Wolters Kluwer – TeamMate e in questo ruolo collabora con i nuovi clienti in Italia e Spagna per aiutarli a valutare le capacità delle soluzioni TeamMate e a capire come la tecnologia può aiutare a soddisfare le esigenze dei loro dipartimenti di Internal Audit.

Prima di questo incarico, ha ricoperto ruoli di lead internal auditor per società quotate italiane nei settori dell'energia e delle infrastrutture. Ha iniziato la sua carriera professionale in KPMG, nelle practice di revisione contabile e Internal Audit, Risk & Compliance. Vanessa è laureata in Scienze Economico-Aziendali e ha completato un Executive MBA al POLIMI Graduate School of Management.

Vanessa Olarte Bendezu, CIA, CFE
Business Solutions Manager
Wolters Kluwer TeamMate
vanessa.bendezu@wolterskluwer.com

Domanda di sondaggio n. 1

Qual è la dimensione del vostro team di audit interno/controllo?

A. 1-5
B. 6-10
C. 10-30
D. +30

Trend e Framework in ambito cyber

Domanda di sondaggio n. 2

Quali sono i 3 principali rischi che la sua organizzazione deve affrontare?

A. Cybersecurity
B. Digital Disruption (inclusa l'IA)
C. Business Continuity
D. Risorse umane
E. Cambiamenti climatici
F. Cambiamenti normativi
G. Incertezza geopolitica
H. Cambiamenti del mercato / Concorrenza
I. Liquidità finanziaria
J. Catena di fornitura
K. Frode

IIA Risk in Focus 2026 – Global – I rischi più elevati secondo i risultati del sondaggio Risk in Focus 2026

Risk Area	Average of the regions	Africa	Asia Pacific	Europe	Latin America	Middle East	North America
Cybersecurity	73%	62%	62%	82%	76%	72%	86%
Digital Disruption (including AI)	48%	44%	39%	47%	54%	50%	53%
Business resilience	47%	49%	58%	39%	35%	58%	46%
Human capital	43%	35%	56%	48%	40%	38%	42%
Regulatory change	41%	34%	38%	45%	49%	28%	51%

- La **cybersecurity** è di gran lunga il rischio più diffuso a livello mondiale (73%)

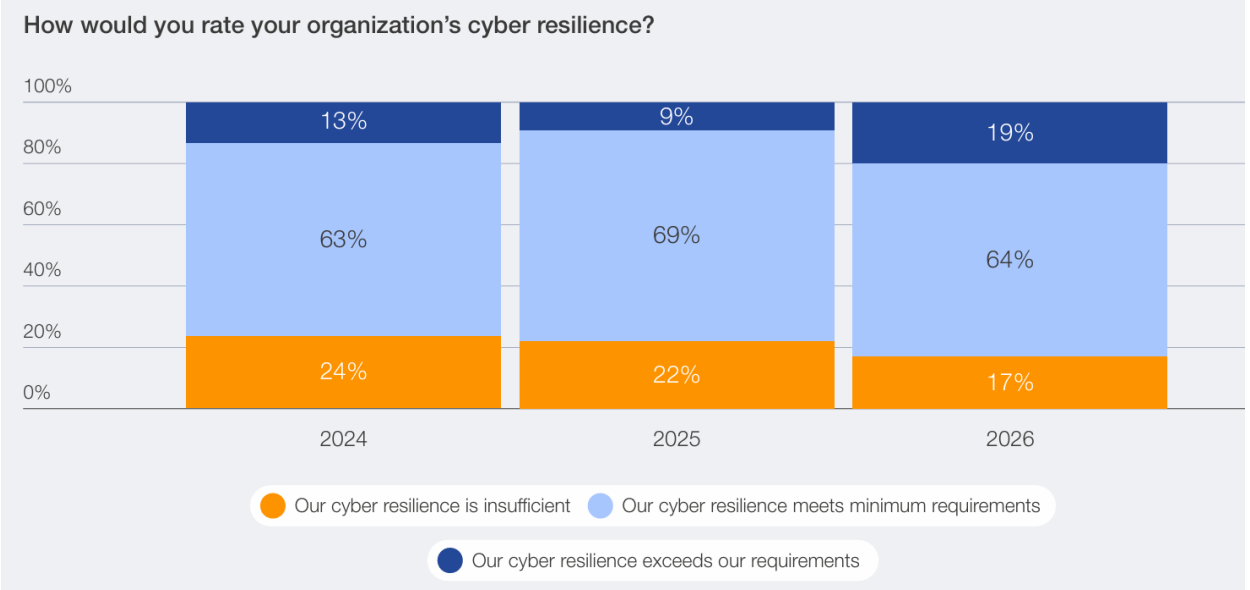
2026 Global Summary Risk in Focus Report English

Il legame tra business resilience e cybersecurity

- Un solido programma di sicurezza informatica è alla base della resilienza operativa di un'organizzazione (Federal Reserve Board)
- La resilienza operativa è la capacità delle organizzazioni di continuare a fornire servizi critici di fronte a minacce in continua evoluzione. La sicurezza informatica è un meccanismo chiave attraverso il quale le organizzazioni raggiungono questo obiettivo (The Berkeley Partnership)

Forum economico mondiale – Prospettive globali sulla sicurezza informatica 2026

- La resilienza informatica è alla base della capacità di un'organizzazione di ridurre al minimo l'impatto di gravi incidenti informatici sui propri obiettivi aziendali primari.
- I dati del sondaggio evidenziano una crescente fiducia nella resilienza informatica delle organizzazioni.
- Si registra un aumento a doppia cifra rispetto al 2025, quando solo il 9% delle organizzazioni dichiarava di aver superato i requisiti di resilienza.



Global Cybersecurity Outlook 2026 | World Economic Forum

I principali attacchi informatici nel mondo nel 2025

Asia-Pacific Cyberattack Highlights

COUNTRY	INCIDENT	IMPACT
Taiwan	960M+ intrusion attempts by Chinese APTs	Energy and healthcare sectors targeted
Japan	Asahi Breweries ransomware attack	Operations suspended; 27GB data stolen
South Korea	Coupang data breach	34M customer records exposed
APAC-wide	16B credential mega leak	Massive credential-stuffing risk

United States Cyberattack Overview

SECTOR	INCIDENT	IMPACT
Telecom	Salt Typhoon infiltration	Verizon, AT&T, Charter compromised
Government	SharePoint supply-chain breach	400+ organizations affected
Healthcare	Covenant Health breach	478K patient records exposed
Finance	ByBit crypto heist	$1.5B stolen by Lazarus Group
Cloud	Oracle SSO/LDAP breach	6M identity records compromised

United Kingdom and European Incidents

COUNTRY	INCIDENT	IMPACT
UK	M&S ransomware attack	£300M losses; retail operations halted
UK	Barts Health NHS breach	Oracle EBS zero-day exploited
Germany/Poland/Finland	VoltBreaker grid attacks	Blackouts across multiple regions
Romania	Energy provider ransomware	ERP and email systems disrupted
Norway	Dam control system hack	Valve manipulation for 4 hours

Come abilitare audit cyber più efficaci e strutturati

Conoscenza del Quadro Normativo di Riferimento

Principali quadri normativi UE

- Il GDPR, la direttiva NIS2 e il DORA definiscono standard completi in materia di sicurezza informatica e protezione dei dati nell'UE.

Requisiti di conformità

- Per essere conformi, le organizzazioni devono implementare notifiche di violazione, DPIA, crittografia e autenticazione a più fattori.

Audit e Governance

- Gli audit interni verificano i controlli di conformità, mentre i consigli di amministrazione garantiscono le strategie di sicurezza informatica e la prontezza nella risposta agli incidenti.

Sanzioni per la non conformità

- La non conformità comporta il rischio di multe fino al 4% del fatturato globale ai sensi del GDPR, sottolineando la responsabilità normativa.

Topical Requirement dell'IIA in materia di cybersecurity

In vigore da febbraio 2026

- Un quadro di riferimento obbligatorio (utilizzato in combinazione con i GIAS) che definisce aspettative minime chiare per auditare gli aspetti relativi ai rischi di sicurezza informatica e migliorare la coerenza e la qualità dei risultati di verifica.
- La conformità è obbligatoria per gli incarichi di audit e raccomandata per gli incarichi di consulenza.
- Una base coerente e fondata su cui valutare se i processi di governance, gestione dei rischi e controllo in materia di sicurezza informatica siano stati progettati e attuati in modo efficace.

IT Audit Framework (ITAF)

- Un quadro di riferimento completo che offre un approccio strutturato agli incarichi di audit e di verifica informatica
- L'ITAF comprende standard e linee guida per incarichi di audit informatico strutturati
- Requisiti minimi e indicazioni pratiche per gli incarichi di audit informatico
- Include una mappatura con il COBIT e il Digital Trust Ecosystem Framework (DTEF)

Informazioni sui principali vettori di attacchi informatici

- **MITRE ATT&CK®:** una base di conoscenze accessibile a livello globale sulle tattiche e le tecniche degli aggressori, basata su osservazioni reali.
- **OWASP Top 10:** documento standard di sensibilizzazione sulla sicurezza delle applicazioni web.
- Seguire i siti web delle agenzie nazionali

Domanda di sondaggio n. 3

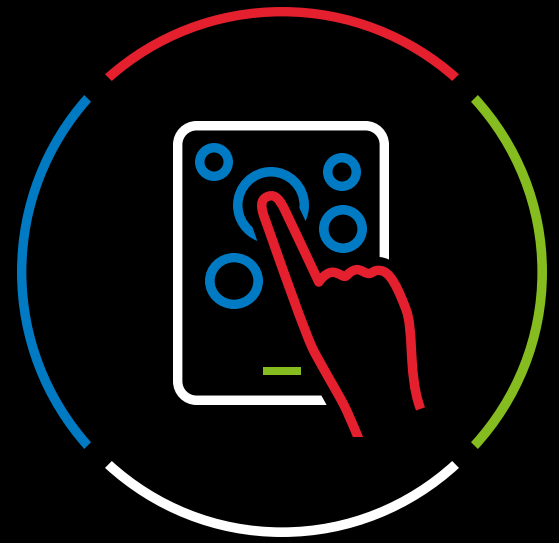
In che misura si ritiene a proprio agio con i modelli di sicurezza informatica e di resilienza operativa?

A. Abbastanza
B. Non ne so molto
C. Un po'
D. Preferisco non rispondere

In che modo la tecnologia può contribuire a migliorare le attività di audit e controllo?

- Definire template e linee guida per cyber audit direttamente all'interno di un tool
- Adottare una metodologia standardizzata e coerente per ridurre il lavoro manuale e documentare ciò che conta davvero
- Archiviare e monitorare tutte le informazioni relative a rischi informatici, controlli, incidenti e fornitori in un'unica piattaforma centralizzata

Approccio pratico (Demo)

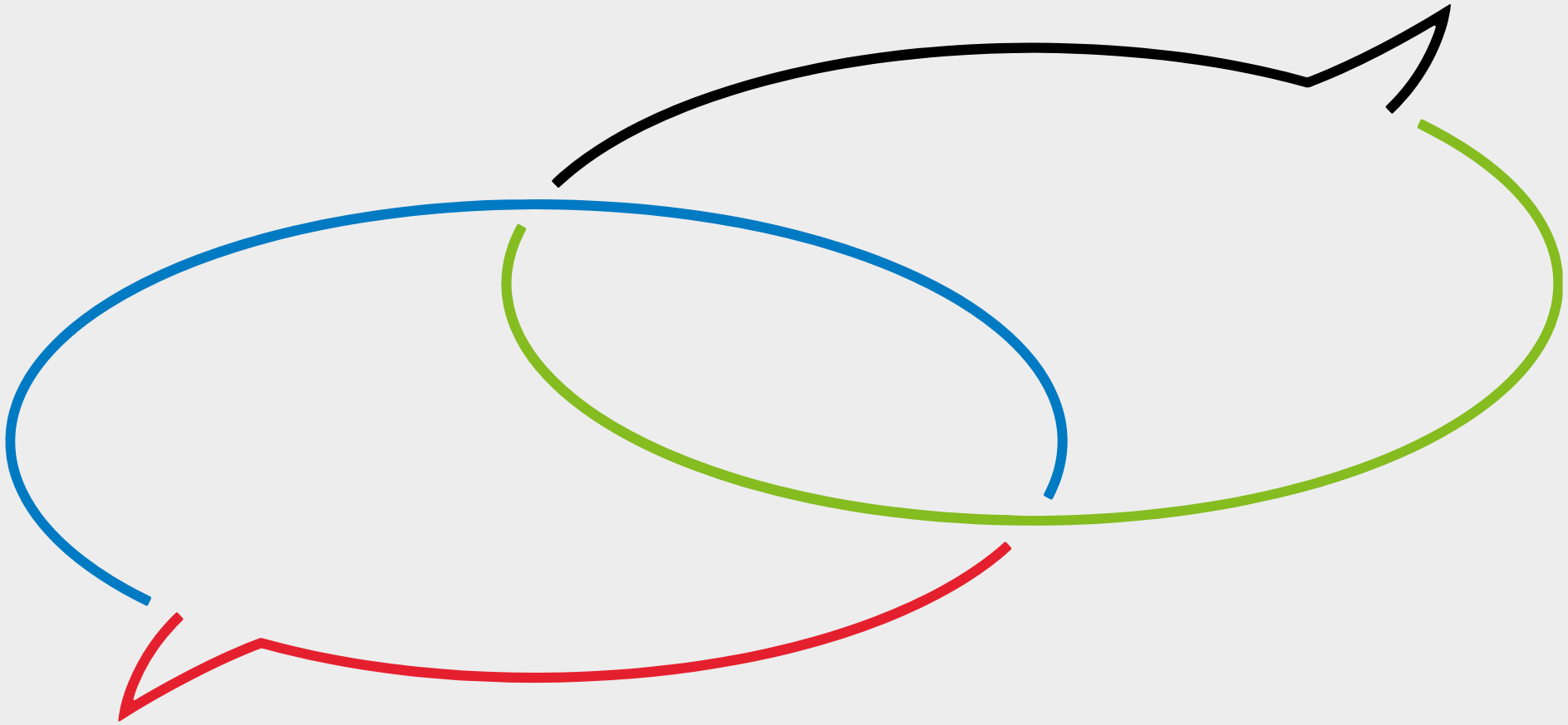


Domanda di sondaggio n. 4

La vostra organizzazione include audit di cybersecurity nel piano di audit?

A. Sì
B. No
C. Non so

Q&A



Grazie