



Associazione Italiana
Internal Auditors

Risk in Focus 2027 e l'evoluzione dei rischi in Europa

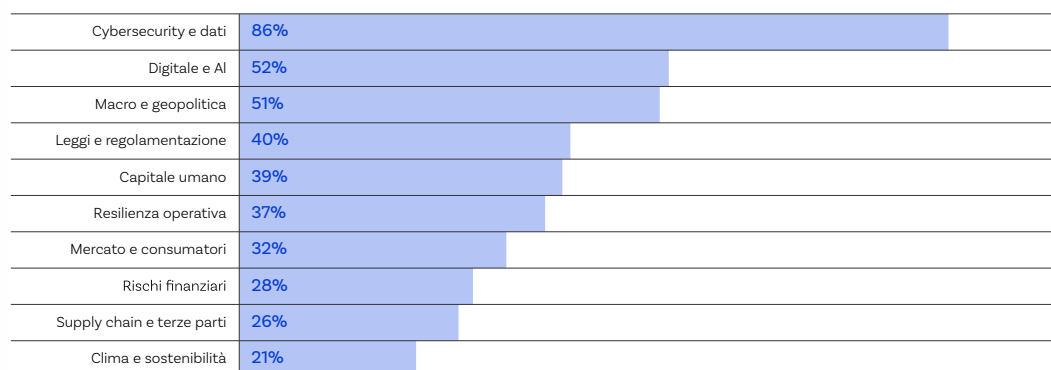
**Driver, impatti e priorità di Audit
nel confronto con l'Italia**

Emanuele Patrini

Partner di Excellence GREG · Gruppo Excellence

Anche per questo report, il punto di partenza è la capacità di leggere il cambiamento attraverso i rischi che le organizzazioni considerano più rilevanti. Il Risk in Focus 2027 conferma la centralità della cybersecurity e mette in evidenza l'avanzata dell'intelligenza artificiale e dell'incertezza geopolitica. Il confronto con le edizioni precedenti e con le risposte italiane permette però di andare oltre l'ordine della classifica, osservando come evolvano le esposizioni e quanto i sistemi di governo e controllo riescano ad accompagnarle.

La ricerca europea raccoglie 797 risposte di Chief Audit Executive, i responsabili delle funzioni di Internal Audit, comprendendo anche il Regno Unito. Considera sedici categorie e affianca alle priorità di rischio la severità percepita, la maturità della gestione e l'impegno dell'Audit. Il quadro si inserisce in una ricerca globale con 3.285 rispondenti in 132 paesi e territori. Qui la lettura europea è integrata con i 99 questionari italiani: le percentuali indicano la frequenza di inclusione fra i cinque rischi principali, non la probabilità di un evento.



Rispondenti che includono il rischio nei primi cinque (%)

Figura 1 · I dieci rischi più segnalati in Europa. Fonte: Risk in Focus 2026/27, p. 6.

Cybersecurity e sicurezza dei dati

Il cyber rimane primo con l'86%. I driver comprendono attacchi più sofisticati, crescente dipendenza digitale, gestione delle identità e degli accessi privilegiati, oltre all'esposizione dei fornitori critici. L'uso dell'AI può amplificare la capacità offensiva e la velocità degli attacchi. Gli impatti investono continuità dei servizi, integrità e riservatezza dei dati, costi di ripristino e fiducia di clienti e stakeholder, con possibili responsabilità e sanzioni.

Le priorità di Audit riguardano l'efficacia dei presidi su identità e accessi, cloud e terze parti, insieme alla risposta agli incidenti e ai test di recupero dei servizi. Il cyber guida anche l'impegno dell'Audit, all'80%, e presenta una maturità di 3,67 su 5. Una risposta relativamente sviluppata deve comunque essere aggiornata alle esposizioni effettive: la continuità dipende anche dalla capacità di ripristinare processi e servizi quando l'incidente nasce fuori dall'organizzazione.

Disruption digitale, nuove tecnologie e intelligenza artificiale

La dipendenza tecnologica che alimenta il rischio cyber si intreccia con la trasformazione dei processi. Digitale e AI raggiungono il secondo posto con il 52%. Fra i driver emergono l'adozione rapida dell'AI generativa, dati frammentati o di qualità incerta, applicazioni sviluppate al di fuori dei percorsi autorizzativi e dipendenza da piattaforme esterne. L'urgenza di innovare può rendere difficile mantenere una visione completa degli strumenti utilizzati e delle responsabilità associate.

Gli impatti riguardano decisioni distorte o poco spiegabili, errori replicati su larga scala, esposizione di informazioni riservate e possibili violazioni di privacy o proprietà intellettuale. A questi si aggiunge il rischio di investimenti che non producono i benefici attesi. La trasformazione modifica, inoltre il lavoro delle persone e può introdurre dipendenze difficili da sostituire, rendendo necessario valutare insieme tecnologia, processi e organizzazione.

Le priorità di Audit partono dalla governance dell'AI: inventario dei casi d'uso, responsabilità, criteri di approvazione e supervisione umana. Proseguono con qualità e provenienza dei dati, validazione dei modelli, controllo dei cambiamenti e monitoraggio del deterioramento delle prestazioni. Il report attribuisce al digitale la maturità più bassa, 2,87 su 5, mentre il 34% lo include fra le principali aree di effort Audit. Il divario segnala quanto sia importante accompagnare l'adozione con lo sviluppo delle capacità di gestione e verifica.

Incertezza macroeconomica, sociale e geopolitica

Alla trasformazione interna si aggiunge l'instabilità del contesto esterno. Il rischio macroeconomico e geopolitico è terzo, al 51%. I driver comprendono conflitti, tensioni commerciali, protezionismo, sanzioni e frammentazione normativa, insieme a inflazione, tassi e volatilità valutaria. Questi fattori possono modificare rapidamente le ipotesi su cui si fondano budget, investimenti e strategie commerciali.

Gli impatti si trasmettono a margini e liquidità, disponibilità e costo delle forniture, rischio paese e controparte. Possono anche rendere meno sostenibili decisioni assunte in condizioni diverse. Le priorità di Audit riguardano la qualità della scenario analysis e degli stress test, la resilienza finanziaria, le esposizioni a paesi e controparti e la gestione delle sanzioni. È rilevante verificare anche le soglie che attivano risposte di crisi e le responsabilità decisionali.

La maturità media è 3,11 su 5 e solo l'8% indica quest'area fra quelle di maggiore effort Audit. Parte delle verifiche può ricadere in tesoreria o supply chain; il dato invita quindi a ricostruire l'assurance complessiva. Rimane essenziale capire se l'incertezza sia tradotta in scenari e decisioni verificabili, anziché restare una premessa generica della pianificazione.

Nuove leggi e regolamentazione

La frammentazione del contesto influenza anche il rischio regolamentare, quarto con il 40%. I driver comprendono l'evoluzione dei requisiti sulla resilienza digitale, richiamati nel report attraverso DORA e NIS2, le regole su AI, dati e privacy, il reporting di sostenibilità e l'attenzione alle terze parti. La complessità cresce quando gli stessi processi devono rispondere a più requisiti e le responsabilità sono distribuite fra funzioni diverse.

Gli impatti possono tradursi in sanzioni e interventi delle autorità, costi di adeguamento, ritardi nelle remediation e responsabilità degli organi aziendali. Duplicazioni e incoerenze fra controlli possono indebolire anche un sistema formalmente completo. Le priorità di Audit riguardano la mappatura dei requisiti applicabili, l'attribuzione delle responsabilità e la corrispondenza fra policy, controlli operativi ed evidenze di conformità, insieme al coordinamento delle funzioni di controllo.

Il presidio appare relativamente consolidato: la maturità è 3,51 su 5 e il 50% colloca la regolamentazione fra le principali aree di impegno Audit. La sua posizione nel ranking richiede però cautela, perché alcune esposizioni normative possono essere classificate dentro cyber, digitale o resilienza. Un cambiamento di frequenza non dimostra, da solo, che la pressione regolamentare sia diminuita.

Capitale umano, competenze e retention

La capacità di rispondere a queste pressioni dipende infine dalle persone. Il capitale umano è quinto al 39%. I driver comprendono carenza di competenze digitali e cyber, turnover nelle funzioni critiche, nuove aspettative sul lavoro e pressione su produttività e costi. La trasformazione tecnologica modifica il fabbisogno di professionalità proprio mentre aumenta la complessità dei processi da governare.

Gli impatti possono manifestarsi come dipendenza da poche figure chiave, perdita di conoscenza organizzativa, rallentamento dei programmi di innovazione e discontinuità nell'esecuzione dei controlli. Le priorità di Audit comprendono pianificazione della forza lavoro, analisi dei gap di competenza, successione e rischio di persone chiave. Vi rientrano anche gestione degli accessi in ingresso e uscita e governo di outsourcing e consulenti, affinché il ricorso all'esterno mantenga la capacità interna di indirizzo e controllo.

La maturità è 3,23 su 5 e la frequenza fra le principali aree di effort Audit è il 22%. Il capitale umano arretra nella classifica, ma continua a condizionare le risposte ai rischi che avanzano. Leggere insieme i cinque temi rende visibile questo legame: innovazione, sicurezza e adattamento al contesto richiedono competenze e responsabilità coerenti. Il confronto storico aiuta a comprendere come si stia redistribuendo l'attenzione su tali fattori.

L'evoluzione delle priorità dal 2025 al 2027

Nel triennio la cybersecurity conserva il primo posto, mentre digitale e AI salgono dal quarto al terzo e poi al secondo. Macroeconomia e geopolitica passano dal quinto posto del 2025 al quarto del 2026, a pari merito con la regolamentazione, per arrivare al terzo. Il capitale umano segue la traiettoria opposta, dal secondo al quinto; clima e sostenibilità scendono dal sesto al decimo e rimangono su quella posizione nell'ultima rilevazione.

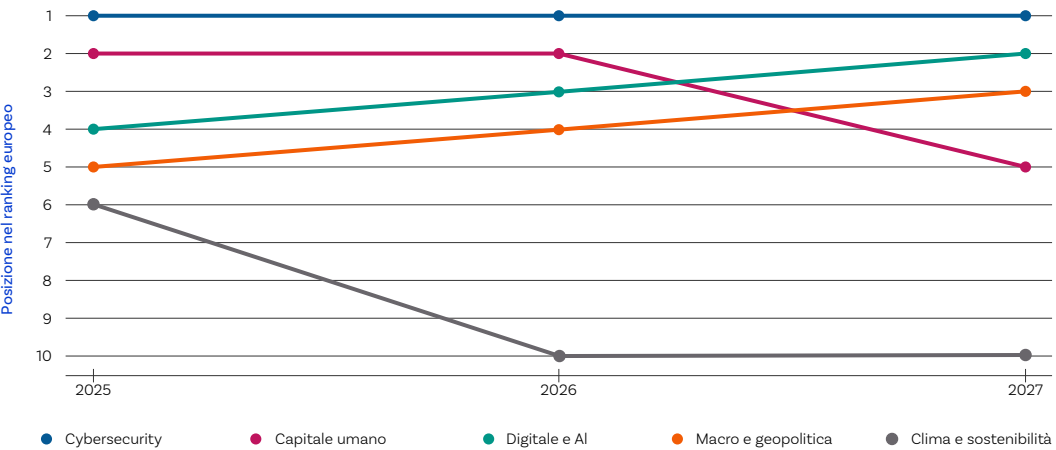


Figura 2 · Evoluzione del ranking europeo. 2027 = edizione 2026/27; nel 2026 macro e regolamentazione sono quarti ex aequo.

Rischio	2025	2026	2027
Cybersecurity e dati	1°	1°	1°
Digitale e AI	4°	3°	2°
Macro e geopolitica	5°	4° ex aequo	3°
Leggi e regolamentazione	3°	4° ex aequo	4°
Capitale umano	2°	2°	5°
Resilienza operativa	7°	6°	6°
Mercato e consumatori	8°	7°	7°
Rischi finanziari	10°	9°	8°
Supply chain e terze parti	9°	8°	9°
Clima e sostenibilità	6°	10°	10°

Tabella 1 · Posizioni nelle tre edizioni. Fonti: presentazione di sintesi e pubblicazioni Chartered IIA ed ECIIA.

La centralità del digitale cresce lungo tutto il periodo, mentre la geopolitica porta nell'agenda aziendale una maggiore attenzione alle condizioni esterne. Altri movimenti sono più gradual: i rischi finanziari avanzano dal decimo all'ottavo posto, la resilienza passa dal settimo al sesto e mercato e consumatori dall'ottavo al settimo. Le classifiche confrontano campioni diversi e descrivono priorità relative, non una misura delle perdite attese.

L'arretramento di capitale umano e clima non implica quindi una riduzione dell'esposizione assoluta. Competenze insufficienti possono indebolire AI e controlli; eventi climatici possono incidere su beni, forniture e continuità. Il benchmark diventa utile quando questi movimenti vengono confrontati con la materialità dell'organizzazione. Le risposte italiane mostrano come la distribuzione delle priorità possa cambiare anche all'interno del quadro europeo.

Il profilo italiano nel confronto con l'Europa

L'Italia condivide le grandi preoccupazioni europee, ma cambia l'ordine dopo il cyber, primo all'81,8%. Macroeconomia e geopolitica sono seconde al 48,5%, davanti al digitale al 45,5% e alla regolamentazione al 43,4%. Mercato e terze parti condividono la quinta posizione al 36,4%; il capitale umano è settimo al 31,3%. Il confronto evidenzia soprattutto il maggiore peso italiano delle dipendenze esterne e di salute e sicurezza.

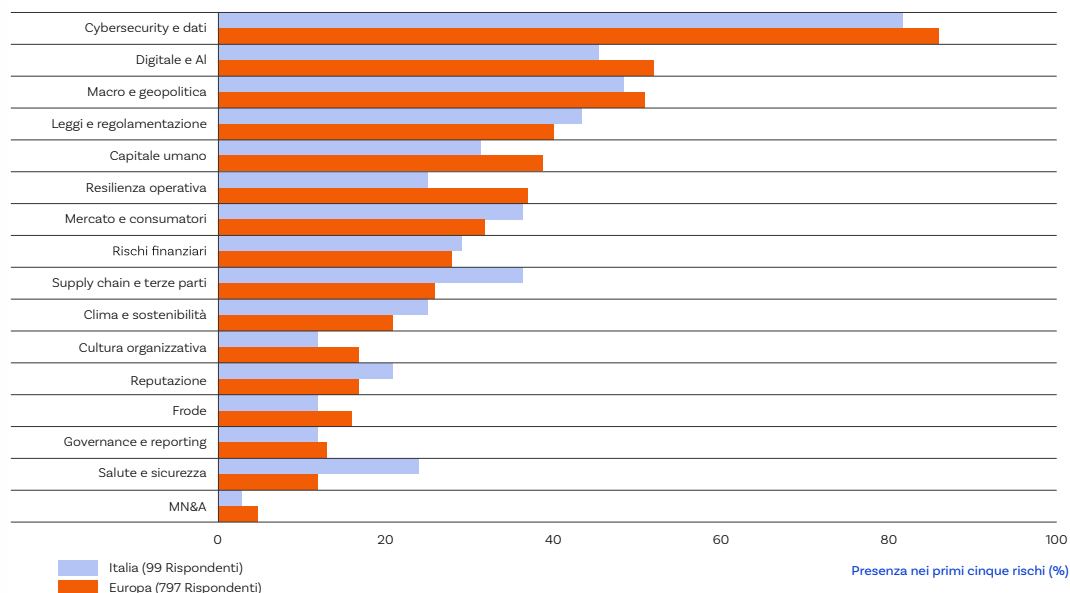


Figura 3 - Presenza fra i primi cinque rischi. Italia: 99 rispondenti; Europa: 797, compresa l'Italia. Fonte: Excel e report europeo.

Categoria di rischio	Italia %	Europa %	Scarto pp
Cybersecurity e dati	81,8	86	-4,2
Digitale e AI	45,5	52	-6,5
Macro e geopolitica	48,5	51	-2,5
Leggi e regolamentazione	43,4	40	+3,4
Capitale umano	31,3	39	-7,7
Resilienza operativa	25,3	37	-11,7
Mercato e consumatori	36,4	32	+4,4
Rischi finanziari	29,3	28	+1,3
Supply chain e terze parti	36,4	26	+10,4
Clima e sostenibilità	25,3	21	+4,3
Cultura organizzativa	12,1	17	-4,9
Reputazione	21,2	17	+4,2
Frode	12,1	16	-3,9
Governance e reporting	12,1	13	-0,9
Salute e sicurezza	24,2	12	+12,2
M&A	3,0	5	-2,0

Tabella 2 - Scarto in punti percentuali, Italia meno Europa. Fonti: Excel, Section 2, righe 11-26, colonna G; report, p. 6.

Le terze parti superano il valore europeo di 10,4 punti e salute e sicurezza di 12,2; la resilienza è inferiore di 11,7 punti. Il campione comprende 31 organizzazioni finanziarie private, 45 degli altri settori privati, 15 pubbliche e 8 fra terzo settore e altre categorie. Gli scarti descrivono i partecipanti e risentono della loro composizione. La maturità del digitale è 2,94 contro 2,87 in Europa: una fragilità condivisa che acquista rilievo osservando il lavoro dell'Audit.

La risposta dell'Internal Audit e le implicazioni di governance

In Italia il cyber guida le priorità di impegno dell'Audit al 73,7%, seguito dalle terze parti al 64,6%, contro il 41% europeo. La sensibilità verso la supply chain trova quindi un riscontro nella copertura. Sul digitale solo il 18,2% lo include fra le cinque aree di maggiore effort, rispetto al 34% europeo, pur considerandolo prioritario nel 45,5% dei casi. Anche la geopolitica riceve una bassa priorità diretta di impegno, al 9,1%.

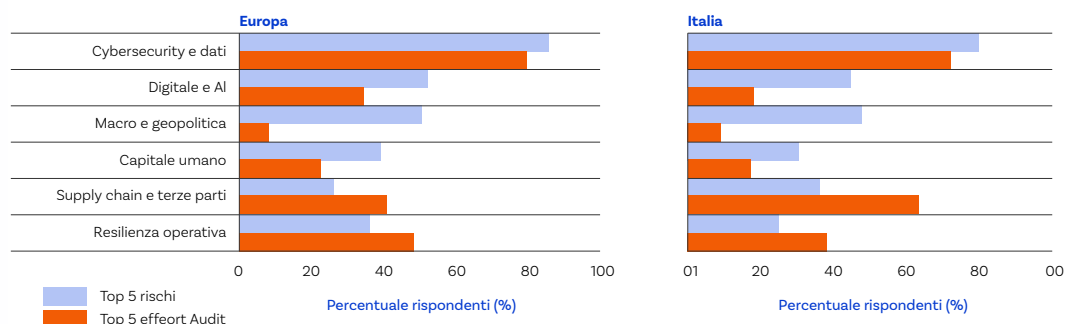


Figura 4 · Top cinque rischi e top cinque aree di effort Audit. Le percentuali non sono quote di ore del piano. Fonti: report, pp. 6-7; Excel.

Area	Effort Italia %	Effort Europa %	Aumento Italia %
Cybersecurity e dati	73,7	80	54,5
Supply chain e terze parti	64,6	41	53,5
Leggi e regolamentazione	54,5	50	33,3
Resilienza operativa	39,4	49	43,4
Digitale e AI	18,2	34	47,5
Macro e geopolitica	9,1	8	19,2
Capitale umano	17,2	22	13,1

Tabella 3 · Aumento: quota italiana che dichiara copertura aumentata nel piano 2026/27 rispetto al 2025/26. Fonte: Excel, Section 2.

La risposta sta cambiando: aumenti di copertura sono dichiarati dal 54,5% sul cyber, dal 53,5% sulle terze parti, dal 47,5% sul digitale e dal 43,4% sulla resilienza. Il dato segnala un movimento dei piani senza misurarne l'ampiezza. Anche la distanza fra rischio ed effort richiede cautela: incarichi su governance, fornitori o processi possono coprire esposizioni classificate altrove. Per valutare eventuali carenze occorre ricostruire le verifiche e il contributo delle altre funzioni.

Il Risk in Focus presenta dunque organizzazioni impegnate a rafforzare la capacità di risposta mentre cambiano tecnologia e contesto. Per organi di governo e Internal Audit il suo contributo consiste nel collegare driver, impatti e copertura dei controlli. Il confronto italiano rende particolarmente visibili le dipendenze esterne e il percorso ancora necessario sul digitale. La qualità della governance si misura nella coerenza fra queste esposizioni, le competenze disponibili e le risposte effettivamente attuate.