

Osservatorio Government

In questo numero:

MAGGIO 2025

Internal Audit

1. Al via la IV Edizione del Tavolo di Lavoro sul Sistema di Controllo Interno nella Pubblica Amministrazione
2. Audit e Cybersecurity: una collaborazione strategica per la resilienza informatica

Digitalizzazione

3. AgID traccia la rotta per l'Intelligenza Artificiale nella Pubblica Amministrazione
4. ACN sollecita le PA Centrali all'impiego dello strumento di valutazione e trattamento del rischio cyber

Fondi UE e PNRR

5. Finanziamenti UE: il dibattito sul post-2027
6. PNRR Watch: uno sguardo concreto su risultati, sfide e prospettive del PNRR
7. Efficacia dei controlli in materia di appalti pubblici e aiuti di Stato nell'ambito del Recovery and Resilience Facility (RFF): analisi della Corte dei conti europea
8. Kohesio: tutti i progetti UE a portata di click

Internal Audit

1. Al via la IV Edizione del Tavolo di Lavoro sul Sistema di Controllo Interno nella Pubblica Amministrazione

28/02/2025

Il Tavolo di Lavoro sul Sistema di Controllo Interno nella Pubblica Amministrazione, oggi alla 4° edizione, nasce nel 2019 dalla collaborazione tra Regione Lombardia, l'Università degli Studi di Milano-Bicocca, Protiviti Government Services e ORAC (Organismo Regionale per le Attività di Controllo della Regione Lombardia) e si propone come spazio di riflessione e confronto tra enti, accademici e professionisti impegnati nel miglioramento del sistema di controllo interno del settore pubblico.

Il Tavolo si inserisce in un percorso virtuoso che Regione Lombardia ha voluto avviare per allineare il proprio sistema di controllo alle *best practices* nazionali ed internazionali in ambito Internal Audit, Risk management e Compliance.

In questa quarta edizione i partecipanti al Tavolo discuteranno l'applicabilità dei nuovi *Global Standard dell'Internal Audit* nella PA, non solo con l'obiettivo di rafforzare l'efficacia dei controlli per strutturare una governance più consapevole, coerente e trasparente, ma anche per verificare l'effettiva applicabilità di tali standard all'interno delle pubbliche amministrazioni, tenendo conto delle differenti specificità che ognuna di esse presenta, cercando misure alternative che possano in egual modo portare all'obiettivo finale.

Riferimenti: Come per le scorse edizioni, alla fine del percorso i risultati saranno raccolti in un report disponibile al seguente link: [Tavolo di Lavoro sul Sistema di Controllo Interno nel Settore Pubblico | Protiviti Italy](#)

2. Audit e Cybersecurity: una collaborazione strategica per la resilienza informatica

04/03/2025

La crescente complessità delle minacce informatiche richiede alle organizzazioni di superare le tradizionali divisioni operative. L'*Internal Audit Foundation* e *AuditBoard*, tramite la loro ricerca congiunta, intitolata *Natural Allies*, evidenziano come una stretta collaborazione tra le funzioni di Internal Audit e Information Security possa rafforzare significativamente la resilienza informatica all'interno delle organizzazioni.

Nel panorama attuale della cybersicurezza, sono tre le modalità di attacco più diffuse: il phishing, l'abuso di credenziali e lo sfruttamento delle vulnerabilità note, ovvero debolezze di sicurezza già identificate e documentate all'interno di software, sistemi operativi o applicazioni. Secondo la ricerca sopra citata, il 73% dei responsabili dell'audit ha inserito il rischio cyber tra i primi cinque rischi, superando di gran lunga il secondo rischio più menzionato, il capitale umano.

Il focus di *Natural Allies* è dunque sottolineare l'importanza di sviluppare un linguaggio comune e obiettivi condivisi tra i due settori, al fine di migliorare l'identificazione e la gestione dei rischi informatici. Tra le strategie pratiche suggerite, le "*Five Emergent Themes*", vi sono la condivisione continua delle informazioni, l'allineamento degli obiettivi, il consolidamento dei rapporti interfunzionali e la formazione congiunta dei team.

Attraverso tavole rotonde virtuali, i leader dell'Internal Audit e dell'Information Security hanno condiviso esperienze concrete, evidenziando come una collaborazione strutturata porti a una maggiore capacità di anticipare e mitigare le minacce, oltre a promuovere una "cultura aziendale" più consapevole e proattiva in materia di cybersecurity.

In generale, lo studio offre spunti preziosi per le organizzazioni che mirano a integrare efficacemente le funzioni di Internal Audit e Information Security, trasformando potenziali vulnerabilità in punti di forza strategici.

Per scaricare il documento completo, clicca [qui](#).

Riferimenti: *Natural Allies: Nurturing Cyber Resilient Cultures Through Internal Audit and Information Security Collaboration | IA Foundation | AIIA*

3. AgID traccia la rotta per l'Intelligenza Artificiale nella Pubblica Amministrazione

18/02/2025

L'Agenzia per l'Italia Digitale (AgID) ha diffuso la bozza delle nuove Linee Guida per l'adozione dell'Intelligenza Artificiale nella Pubblica Amministrazione, un documento strategico pensato per accompagnare gli enti pubblici nel percorso di trasformazione digitale in modo etico, sicuro e sostenibile. L'obiettivo delle linee guida è quello di integrare l'IA nelle PA come un processo strategico, dinamico e orientato al miglioramento continuo, capace di adattarsi alle esigenze in evoluzione del settore pubblico.

Il modello proposto si basa su pilastri fondamentali:

- la definizione di una strategia coerente con la missione e le funzioni dell'ente,
- la valorizzazione dei dati,
- la formazione del personale,
- la sperimentazione guidata su casi d'uso a basso rischio.

L'intelligenza artificiale viene così presentata come una leva per snellire i processi interni (come la gestione documentale e il supporto decisionale), offrire servizi personalizzati e accessibili ai cittadini, e rafforzare la sicurezza informatica e la tutela dei dati.

Ogni PA è invitata ad avviare una riflessione interna per valutare i propri bisogni, definire le priorità e attivare un coordinamento strutturato con il Responsabile della Transizione Digitale (RTD), il Responsabile della Protezione dei Dati (RPD) e gli altri attori istituzionali, in coerenza con il Piano Triennale per l'Informatica nella PA.

La consultazione pubblica sul documento si è conclusa il 20 marzo. La versione definitiva delle Linee Guida, attesa prossimamente, rappresenterà un punto di riferimento essenziale per un'adozione dell'IA trasparente, efficace e a misura di cittadino.

Riferimenti: *Intelligenza Artificiale: in consultazione le prime Linee Guida per la PA | Agid*

4. ACN sollecita le PA Centrali all'impiego dello strumento di valutazione e trattamento del rischio cyber

25/02/2025

Le crescenti tensioni geopolitiche, l'espansione delle tecnologie digitali attraverso dispositivi connessi, l'uso di questi strumenti in mobilità, la pratica del *Bring Your Own Device* (utilizzo del dispositivo personale in ambito aziendale) e la crescente minaccia da parte dei cybercriminali, aumentano il rischio digitale e impongono un approccio innovativo alla resilienza e alla sicurezza informatica. In questo contesto, l'Agenzia per la Cybersicurezza Nazionale (ACN) invita le Pubbliche Amministrazioni Centrali ad adottare un approccio innovativo e sistemico alla gestione del rischio cibernetico, riconosciuto come leva strategica per costruire una cultura della resilienza e rafforzare la sicurezza del perimetro digitale nazionale.

Per sostenere questo processo, l'ACN ha messo a disposizione delle PA uno strumento operativo per l'identificazione, analisi, valutazione e trattamento dei rischi informatici, aggiornato periodicamente in base all'evoluzione delle minacce. Lo strumento fornisce una guida metodologica allineata ai principali standard internazionali di sicurezza (come ISO/IEC 27005 sulla gestione del rischio informatico e NIST Cybersecurity Framework), e si articola lungo tutte le fasi del ciclo di gestione del rischio: dalla mappatura delle vulnerabilità, alla definizione dei piani di mitigazione, fino al monitoraggio continuo degli scenari di rischio.

L'obiettivo è duplice: potenziare le competenze cyber all'interno della PA e favorire una *governance* del rischio proattiva, in linea con le direttive europee come la NIS2 (Network and Information Security Directive), che impone nuovi obblighi di sicurezza e gestione del rischio agli enti pubblici e privati strategici.

Riferimenti: *Rischio cyber - ACN invita le Pubbliche Amministrazioni Centrali all'utilizzo dello strumento di valutazione e trattamento del rischio cyber - ACN*

FONDI UE E PNRR

5. Finanziamenti UE: il dibattito sul post-2027

20/02/2025

Nel contesto del dibattito sul futuro dei finanziamenti europei dopo il 2027, il Parlamento europeo ha pubblicato lo studio *“A renewed long-term budget for the Union in a changing world”*, un’analisi approfondita sulle sfide che attendono l’Unione, sulle politiche da mettere in campo e sulle risorse necessarie per sostenerle.

Lo scenario globale è complesso e in continua evoluzione: dal sostegno all’Ucraina al rilancio degli investimenti in difesa, dalla transizione verde e digitale al rimborso del debito contratto per finanziare le sovvenzioni del programma Next Generation EU. In questo contesto, i bilanci nazionali degli Stati membri sono sottoposti a vincoli sempre più stringenti, rendendo ardua la definizione di un Quadro Finanziario Pluriennale (QFP) capace di bilanciare priorità comuni e interessi nazionali.

Uno dei punti centrali sollevati dal Parlamento è la necessità che il QFP post-2027 sia dotato di maggiore flessibilità e di margini di bilancio più ampi, per permettere all’Unione di rispondere con tempestività alle crisi e alle esigenze emergenti. Viene inoltre sollevata la questione della possibilità di un indebitamento comune, da valutare sotto condizioni precise, come strumento potenziale per sostenere la crescita economica e preservare la stabilità dei conti pubblici.

Clicca [qui](#) per scaricare il documento completo.

Riferimenti: <https://www.tecnostruttura.it/news.php?id=1828>

6. PNRR Watch: uno sguardo concreto su risultati, sfide e prospettive del PNRR

06/03/2025

Con oltre 200 miliardi di euro destinati a sei ambiti di intervento strategico, il PNRR rappresenta una delle più grandi opportunità per il rilancio economico e sociale dell’Italia nel contesto post-pandemico. Affinché il piano abbia un impatto reale sul tessuto socioeconomico del Paese e rispetti gli impegni presi in sede europea è fondamentale garantirne la trasparenza, la responsabilità e il controllo pubblico.

Il PNRR Watch, progetto firmato *Assonime* e *Openpolis*, mette sotto la lente alcuni degli investimenti più strategici del piano, con l’obiettivo di valutarne impatti reali, criticità e prospettive future. Il focus iniziale è sulla Digitalizzazione della Pubblica Amministrazione e infrastrutture per la connettività, due pilastri fondamentali per la modernizzazione del Paese.

Si tratta di un vero e proprio osservatorio editoriale nato per raccontare – con dati, analisi e approfondimenti – come il Piano stia prendendo forma. Ogni uscita è dedicata a misure chiave, valutandone l’efficacia concreta e individuando possibili ostacoli alla loro realizzazione. Sono sei gli interventi analizzati in questa prima uscita, per un valore complessivo di oltre 7 miliardi di euro. Tra questi, la creazione del Polo Strategico Nazionale, il supporto alla migrazione in cloud della PA locale e la Piattaforma Digitale Nazionale Dati.

Riferimenti: <https://www.openpolis.it/nasce-pnrr-watch-per-un-monitoraggio-sulla-transizione-digitale-dellitalia/>

7. Efficacia dei controlli in materia di appalti pubblici e aiuti di Stato nell’ambito del Recovery and Resilience Facility (RRF): analisi della Corte dei Conti europea

10/03/2025

La Relazione speciale 09/2025 della Corte dei Conti europea esamina l’efficacia dei sistemi di controllo interno degli Stati membri dell’UE sul rispetto delle norme in materia di appalti pubblici e aiuti di Stato nell’ambito del dispositivo per la ripresa e la resilienza (RRF).

Se da un lato i progressi negli audit condotti dalla Commissione sono evidenti, dall'altro la Corte mette in luce significative lacune nei sistemi di monitoraggio degli Stati Membri. L'analisi approfondita ha coinvolto un campione di 5 Stati Membri (Croazia, Cechia, Francia, Italia, Spagna), mostrando come, in alcuni casi, i controlli siano insufficienti o scarsamente documentati, mettendo a rischio la corretta gestione dei fondi.

Tra le principali raccomandazioni, la Corte invita:

- la Commissione europea a rafforzare i propri controlli e a garantire un maggior coordinamento con le autorità nazionali,
- gli Stati Membri a potenziare i meccanismi di trasparenza e accountability, adottando strumenti digitali e pratiche di auditing più rigorose,
- la stessa UE a fornire linee guida più chiare e vincolanti per assicurare l'osservanza delle norme in tutte le fasi della gestione del RRF, dalla pianificazione all'attuazione.

La Corte richiama l'attenzione sull'urgenza di standard più omogenei a livello europeo, capaci di prevenire distorsioni nella concorrenza e garantire una gestione responsabile e trasparente delle risorse comuni. In caso di violazioni, sottolinea l'importanza di attuare misure correttive efficaci e proporzionate, in linea con i principi di legalità, efficienza ed equità.

Riferimenti: [NEWS-SR-2025-09 | European Court of Auditors](#)

8. Kohesio: tutti i progetti UE a portata di click

20/03/2025

Era il marzo del 2022 quando la Commissione europea lanciò la piattaforma “Kohesio”, al fine di raccogliere più informazioni possibili sui progetti in corso di realizzazione negli Stati Membri finanziati dalla Politica di coesione nella Programmazione 2014-2020. L'accesso alle informazioni risulta estremamente semplice: attraverso l'utilizzo di una mappa interattiva è possibile accedere ai dati in formato *open data* cliccando sul Paese di interesse.

Il sito e la piattaforma sono gestiti dalla Direzione Generale per la Politica Regionale e Urbana della Commissione europea ed è disponibile in tutte le lingue ufficiali dell'Unione.

Su Kohesio è possibile navigare ed effettuare ricerche tematiche su:

- dati standardizzati relativi ai singoli progetti, compresi i link ai rispettivi programmi e fondi;
- dati standardizzati riguardanti i beneficiari dei progetti e stato di avanzamento dei progetti;
- dati relativi a più di 300 programmi operativi in tutti i 27 Stati membri;
- mappa interattiva che consente di recuperare i dati geograficamente.

A partire dallo scorso mese di marzo, è stata introdotta una nuova mappa di navigazione per facilitare il livello di dettaglio e consentire un accesso più rapido ai progetti. Gli utenti potranno inoltre accedere allo spazio per poter modificare la descrizione del progetto, oltre a fornire contenuti aggiuntivi. Infine, dal mese di aprile sono stati inclusi sulla piattaforma anche i nuovi progetti relativi alla Programmazione 2021-2027.

Riferimenti: “Kohesio”: la piattaforma dei progetti finanziati dalla politica di coesione, *OpenCoesione - Kohesio*, <https://www.tecnostuttura.it/news.php?id=1850>

Contatti

Alessandro Cencioni

Managing Director

alessandro.cencioni@protiviti.it

Valentina Cattaneo

Senior Manager

valentina.cattaneo@protiviti.it

Nicola Frascà

Senior Manager

nicola.frasca@protiviti.it