Insights

protiviti®
Global Business Consulting

Internal Audit

Aprile 2025

a cura di:

Francesco Monini
Managing Director

Riccardo Confalonieri
Associate Director

Mattia Santi
Manager

Rischi emergenti: il ruolo dell'Internal Audit nell'era di Crypto & Blockchain

L'adozione dei crypto-asset e della blockchain sta trasformando il settore finanziario.

Dall'evoluzione del contesto normativo, con MiCAR e DORA, alla necessità di nuovi strumenti di controllo, le funzioni Internal Audit devono ripensare il proprio approccio alla gestione del rischio.

Per l'Internal Audit, ciò significa sviluppare nuove competenze, strumenti di monitoraggio avanzati e strategie di governance per affrontare i rischi emergenti con un approccio strutturato e proattivo.

Le sfide regolamentari

Sono passati quasi 5 anni da quando la Commissione Europea, il 24 settembre 2020, ha presentato il Pacchetto sulla Finanza Digitale.

L'obiettivo del Pacchetto è stato quello di colmare una lacuna nella legislazione allora vigente dell'UE, assicurando che il quadro giuridico non ostacolasse l'uso di nuovi strumenti finanziari digitali e, al contempo, garantendo che tali tecnologie e prodotti rientrassero nell'ambito della regolamentazione finanziaria e dei meccanismi di gestione del rischio operativo delle imprese attive nell'UE.

In questo contesto sono recentemente stati emanati il Markets in Crypto-Assets Regulation (MiCAR)[1] e il Digital Operational Resilience Act (DORA)[2], entrati in vigore rispettivamente il 30 dicembre 2024 e il 17 gennaio 2025.

MiCAR

MiCAR si propone di regolamentare tecnologie come blockchain e Distributed Ledger Technologies (DLT), ridurre la frammentazione normativa in Europa e introdurre una regolamentazione armonizzata e chiara. I suoi obiettivi principali includono la protezione dei consumatori e dei partecipanti al mercato, la tutela dell'integrità del mercato, il mantenimento della stabilità finanziaria e la salvaguardia della sovranità monetaria europea, potenzialmente minacciata dalla crescita incontrollata dei crypto-asset.

MiCAR crea un quadro normativo unificato per i crypto-asset che non rientrano nella legislazione finanziaria già esistente nell'UE, come gli E-Money Token (EMT), gli Asset-Referenced Token (ART) e gli Utility Token. La normativa introduce regole dettagliate, che variano in base alla tipologia di crypto-asset, riprendendo, replicando, combinando normative europee già consolidate, come MiFID, il Regolamento Prospetto e le regole sugli abusi di mercato, oltre a quelle applicabili ai prestatori di servizi di pagamento e agli emittenti di moneta elettronica e finendo per applicare regole e principi propri degli strumenti finanziari e della moneta elettronica ad assets asseritamente non finanziari.

Rispetto a questo quadro normativo, già consolidato e ben noto, MiCAR si propone di affermarsi come un corpus regolamentare autonomo e parallelo, con una propria struttura, portata e disciplina.

DORA

DORA, invece, è stato concepito per armonizzare le norme e i requisiti relativi alla resilienza operativa per il settore finanziario in tutta l'UE, coprendo oltre 20 tipi diversi di entità finanziarie destinatarie, tra cui i Crypto Asset Service Providers (CASP) e i fornitori di servizi ICT di terze parti.

DORA mira a rafforzare la sicurezza informatica e la resilienza operativa del sistema finanziario europeo nel suo complesso. A tal fine, prevede che i CASP monitorino l'intera infrastruttura IT, inclusi i fornitori terzi, identificando le vulnerabilità e implementando strategie solide per proteggere i loro sistemi, i loro dati e i loro clienti.

L'intervento della Funzione Internal Audit è quindi volto a garantire che le organizzazioni non solo rispettino le normative attuali, ma siano anche in grado di adattarsi rapidamente ai cambiamenti normativi e tecnologici che ne conseguono.

Ad esempio, l'Internal Audit gioca un ruolo cruciale per i Crypto Asset Service Providers: secondo la proposta dell'Institute of Internal Auditors (IIA) al Congresso USA del maggio 2023, le linee guida della Financial Conduct Authority (FCA) UK, la normativa emanata dalla Virtual Assets Regulatory Authority (VARA) emiratina nel 2023 e il Decreto Legislativo 27 dicembre 2024, n. 204 di recepimento del Regolamento (UE) 1113/2023 (TFR), è richiesto ai CASP di dotarsi di una Funzione Internal Audit che verifichi nel continuo l'adeguatezza dell'assetto organizzativo e la conformità normativa, con particolare riferimento alle tematiche AML/CFT.

Allo stesso modo, DORA prevede la necessità che l'Internal Audit conduca regolarmente test sui sistemi e infrastrutture ICT per valutarne tanto le vulnerabilità quanto l'efficacia delle misure di protezione adottate.

[1] *Regolamento (UE) 1114/2023*

[2] *Regolamento (UE) 2022/2554*

Decifrare la tecnologia

Per rispondere alle sfide presentate da questo contesto, la conoscenza della tecnologia sottostante diventa imprescindibile. Al centro di questa rivoluzione digitale vi è la blockchain, un registro decentralizzato che alimenta i crypto-asset come i Bitcoin. A differenza dei sistemi finanziari tradizionali, la blockchain opera senza autorità centrali, affidandosi a meccanismi di consenso che garantiscono l'integrità delle transazioni.

Tuttavia, l'immutabilità dei record sulla blockchain, se da un lato garantisce trasparenza e sicurezza, dall'altro rappresenta una sfida per la Funzione Internal Audit, che si può trovare a verificare transazioni su un registro pubblico e potenzialmente infinito.

L'adozione degli smart contract[3] introduce automazione ed efficienza, ma apre anche nuove sfide in termini di sicurezza dal momento che vulnerabilità nel codice, errori di programmazione ed exploit possono essere sfruttati da attori malevoli, con conseguenze potenzialmente devastanti.

Inoltre, la crescente digitalizzazione e la decentralizzazione espongono il settore a nuove minacce informatiche, tra cui attacchi hacker, interruzioni operative e frodi su larga scala.

Un nuovo paradigma per la Funzione Internal Audit nell'identificazione dei Key Risk e nella definizione dell'Audit Universe

L'ecosistema dei crypto-asset è caratterizzato da un alto contenuto tecnologico e presenta tanto rischi comuni con il mondo finanziario tradizionale – sebbene con prospettive differenti – quanto rischi completamente nuovi.

Di seguito, alcuni degli aspetti chiave che le Funzioni Internal Audit devono tenere in considerazione:

1. Framework regolamentare

Sebbene a livello europeo MiCAR sia completamente applicabile dal 30 dicembre 2024, il quadro regolamentare è tutt'ora in evoluzione.

Il suo adeguamento rappresenta una sfida significativa per i CASP italiani ed europei, poiché i requisiti normativi e le aspettative delle autorità di regolamentazione europee sono più stringenti rispetto agli standard attualmente in vigore. Tra gli ambiti di adeguamento più rilevanti possiamo citare: trasparenza e correttezza, best execution, requisiti prudenziali, governance, segregazione tra crypto-asset e fondi dei clienti, reclami, conflitti di interesse, abusi di mercato, esternalizzazione, gestione rischi ICT.

Per garantire una transizione graduale, è stato previsto un periodo transitorio; infatti, i CASP che operavano in conformità alla normativa vigente prima del 30 dicembre 2024 potranno continuare a offrire servizi fino al 1° luglio 2026, o fino al rilascio o al rifiuto dell'autorizzazione MiCAR.

In questo scenario, la Funzione Internal Audit deve assumere un ruolo strategico, supportando le organizzazioni nell'analisi della fattibilità regolamentare, nella valutazione dei rischi dei nuovi prodotti e servizi e nell'implementazione di adeguati presidi di controllo.

2. On-chain monitoring investigation: Market Surveillance & AML/CFT & FS Risks

La trasparenza della blockchain offre opportunità senza precedenti per il monitoraggio del mercato, ma introduce anche sfide complesse. Le transazioni su blockchain, pubbliche e immutabili, richiedono strumenti avanzati capaci di analizzare in tempo reale l'attività on-chain e, al contempo, integrare dati off-chain e fonti OSINT (Open Source Intelligence) per identificare e clusterizzare gli address, rilevando schemi sospetti legati a manipolazione di mercato, frodi, AML/CFT/FS e rischi per la stabilità finanziaria.

[3] *Per smart contract si fa riferimento a "contratti intelligenti" costituiti da un codice crittografico che vengono utilizzati per automatizzare l'esecuzione di un accordo in modo che tutti i partecipanti possano essere immediatamente certi dell'esito, senza intermediari e senza perdite di tempo*

Spesso si tende a credere che i crypto-asset garantiscano un anonimato assoluto, mentre in realtà la natura pubblica e tracciabile della blockchain consente agli investigatori di risalire alle transazioni e ai soggetti coinvolti, soprattutto nel momento in cui i crypto-asset raggiungono un CASP, ossia un ente regolato e soggetto agli obblighi AML. Tuttavia, il fenomeno dei mixer e dei CoinJoin, strumenti utilizzati per offuscare la provenienza dei fondi, rappresenta una criticità significativa.

Questi strumenti complicano le analisi forensi, richiedendo più tempo, risorse e l'impiego di soluzioni avanzate di blockchain analytics per ricostruire il flusso dei crypto-asset. Sebbene in molti casi sia possibile de-mixare le transazioni, l'uso intensivo di questi strumenti può rendere estremamente complesso, se non impossibile, il completo tracciamento dei fondi illeciti.

Sul fronte della stabilità finanziaria, invece, i crypto-asset possono essere utilizzati per aggirare i canali tradizionali di finanziamento, in particolare quelli legati al dollaro statunitense e ai sistemi di pagamento regolamentati. Questo fenomeno si osserva, ad esempio, nei mercati emergenti e nei contesti soggetti a sanzioni economiche, dove i crypto-asset possono diventare un'alternativa alle infrastrutture bancarie tradizionali.

Per mitigare questi rischi, è essenziale un approccio olistico e proattivo, in cui il monitoraggio on-chain sia arricchito dall'analisi di dati off-chain, come informazioni KYC, social network e pattern di comportamento, per migliorare l'attribuzione degli address e la rilevazione di connessioni tra entità.

In questo contesto, le Funzioni Internal Audit devono sviluppare una profonda conoscenza dei tool di monitoraggio blockchain, combinando soluzioni open source e proprietarie con tecniche investigative avanzate di analisi dei dati per garantire un'identificazione tempestiva delle minacce. Solo attraverso una sorveglianza integrata, che unisca le componenti di monitoraggio on-chain, off-chain e OSINT, è possibile rilevare anomalie, anticipare le minacce emergenti e rafforzare la resilienza dell'ecosistema crypto, offrendo opportune garanzie ai clienti e agli stakeholder regolamentari.

3. Crypto-asset Due Diligence

Definire processi rigorosi di due diligence sui crypto-asset è fondamentale per mitigare i rischi legati ai processi di listing[4]. Infatti, la mancata verifica di un crypto-asset può esporre i CASP a rischi normativi, frodi, perdite finanziarie e danni reputazionali.

MiCAR, in questo senso, richiede ai CASP – prima di ammettere un crypto-asset alla negoziazione sulla sua piattaforma – di verificare che lo stesso rispetti le norme operative della piattaforma e di condurre una valutazione strutturata della sua adeguatezza[5].

In questo senso, le Funzioni Internal Audit devono adottare un approccio strutturato per verificare attraverso approfondite due diligence che il processo di listing tenga conto di alcuni rilevanti elementi chiave, tra cui:

- composizione ed esperienza del team di sviluppo,
- White Paper e compliance ai requisiti MiCAR,
- potenziale associazione ad attività illecite o fraudolente, verificando i dati on-chain e off-chain,
- tokenomics e struttura economica,
- sicurezza del codice (smart contract security audit),
- classificazione normativa del crypto-asset,
- coinvolgimento della community e presenza sui social media,
- storico di mercato e pattern di trading.

4. Custodia e Gestione delle Chiavi Private

Le chiavi private sono il fulcro della sicurezza dei crypto-asset dal momento che proteggono l'accesso e l'autorizzazione delle transazioni. Nei CASP, a differenza della finanza decentralizzata (DeFi), le chiavi private dei crypto-wallet non sono gestite direttamente dagli utenti, ma dalla piattaforma stessa.

[4] *MiCAR, ad esempio, richiede che i CASP si dotino di processi di approvazione dei crypto-asset. In caso di violazioni sono previste sanzioni fino a EUR 5 milioni o al 5% del fatturato globale annuo*

[5] *In tal senso anche la Guidance Regarding Listing of Virtual Currencies del 15 Novembre 2025 del New York State Department of Financial Services*

Una compromissione delle chiavi private, dovuta a frodi, furti o attacchi informatici, può esporre gli asset a gravi rischi operativi e finanziari. È quindi essenziale che i CASP adottino solide strategie di custodia, implementando procedure di conservazione sicura delle chiavi private e dei relativi backup.

In questo contesto, le Funzioni Internal Audit devono verificare che siano presenti controlli adeguati lungo l'intero ciclo di vita della chiave privata, assicurando che tutte le fasi critiche – dalla creazione, all'archiviazione, all'utilizzo e alla distruzione – siano gestite secondo best practice di sicurezza.

5. Asset Valuation & Proof of Reserves

Nei CASP, la gestione delle chiavi private implica anche la custodia degli asset degli utenti, creando un parallelismo con il settore bancario per quanto riguarda i depositi. Tuttavia, data l'elevata volatilità e la natura decentralizzata dei crypto-asset, la loro valutazione contabile rappresenta una sfida complessa per gli auditor.

Uno strumento fondamentale per garantire la trasparenza finanziaria è la Proof of Reserves, un processo di verifica che consente ai CASP di dimostrare di possedere fondi sufficienti per coprire i prelievi degli utenti. Tale processo, condotto da un auditor terzo indipendente, prevede:

- verifica dell'effettiva detenzione dei crypto-asset dichiarati dal CASP;
- controllo della corrispondenza tra i saldi degli utenti e le attività di riserva disponibili;
- attestazione che il CASP sia in grado di coprire integralmente i prelievi richiesti dagli utenti.

Affinché la Proof of Reserves sia efficace, deve essere eseguita con metodologie affidabili e trasparenti, evitando tecniche fuorvianti come la presentazione temporanea di fondi ("asset shuffling"). Le Funzioni Internal Audit devono essere in grado di valutare la robustezza del processo, garantendo che la metodologia utilizzata sia conforme agli standard di auditing e best practice di settore.

6. Cybersecurity & ICT

Il settore crypto è stato fin dai suoi albori costantemente minacciato da attacchi informatici, come hacking, phishing e ransomware, con perdite che in alcuni casi hanno superato il miliardo di dollari.

In questo contesto, le Funzioni Internal Audit giocano un ruolo chiave nel valutare e rafforzare le misure di cybersecurity, concentrandosi sulla protezione dei crypto-asset e sulla gestione sicura delle chiavi private. Questo richiede una stretta collaborazione con le funzioni IT & Cybersecurity.

Con l'introduzione di DORA, l'Internal Audit assume un ruolo chiave nella verifica della governance ICT, della gestione dei rischi informatici e delle strategie di risposta e ripristino. Inoltre, deve assicurare audit indipendenti sulla resilienza operativa, inclusi i Threat-Led Penetration Tests (TLPT).

DORA impone inoltre alla Funzione Internal Audit di garantire controlli periodici e un efficace follow-up delle azioni correttive, rafforzando la capacità dell'organizzazione di prevenire e rispondere alle minacce cyber in un contesto digitale sempre più complesso.

7. Privacy

La trasparenza della blockchain è al tempo stesso una risorsa e una criticità: ogni transazione è pubblica e accessibile a chiunque abbia una connessione internet. Tuttavia, l'applicazione di normative sulla privacy come il GDPR impone la protezione dei dati personali, creando una tensione tra la trasparenza della tecnologia e il diritto alla riservatezza.

Le Funzioni Internal Audit devono quindi valutare come vengono gestiti i dati sulla blockchain, garantendo che le soluzioni adottate – come il ricorso a tecnologie di privacy-preserving (es. zero-knowledge proofs) o strumenti di pseudonimizzazione – siano conformi ai requisiti normativi. Inoltre, la Travel Rule[6], introdotta dal FATF, impone l'obbligo per i CASP di raccogliere e condividere informazioni sugli utenti coinvolti nelle transazioni, rendendo ancora più complesso il bilanciamento tra compliance normativa e tutela della privacy.

[6] *Regolamento UE 2023/1113*

In questo contesto, l'Internal Audit gioca un ruolo chiave nel verificare che le strategie di governance dei dati rispettino sia la necessità di trasparenza della blockchain, sia gli obblighi di protezione dei dati personali, assicurando che l'azienda adotti misure adeguate a ridurre i rischi di non conformità e violazione della privacy.

8. ESG

I CASP devono affrontare anche le sfide legate ai criteri ESG. MiCAR, ad esempio, impone l'obbligo di rendere pubbliche le informazioni sui principali impatti climatici e sugli effetti ambientali derivanti dal meccanismo di consenso utilizzato per emettere e validare i crypto-asset su cui i CASP operano.

Le Funzioni Internal Audit devono quindi valutare se le pratiche aziendali siano allineate agli obiettivi ESG, monitorando sia la trasparenza delle dichiarazioni ambientali che l'effettiva sostenibilità operativa. Ciò include la verifica dell'impatto energetico prodotto dai protocolli blockchain adottati, la conformità ai requisiti di disclosure previsti da MiCAR e l'adozione di strategie di mitigazione ambientale, come l'utilizzo di meccanismi di consenso a basso consumo energetico o l'adesione a iniziative di carbon offset.

9. Third Party Vendor Risk

La gestione del rischio legato alle terze parti è fondamentale nel settore crypto, data la frammentazione del panorama dei vendor di blockchain analytics tool[7] e la loro recente evoluzione, trattandosi perlopiù di realtà emergenti sviluppatesi negli ultimi anni.

Per mitigare i rischi associati, le Funzioni Internal Audit devono assicurarsi che il processo di selezione dei fornitori sia ben definito e documentato, valutando parametri tecnici come le regole sottostanti i meccanismi di monitoraggio on-chain, la possibilità di personalizzazione delle regole sottostanti, la competenza del team, l'affidabilità finanziaria e i costi.

Con l'entrata in vigore di DORA, inoltre, i CASP devono adottare un approccio basato sul rischio nella gestione dei fornitori ICT, garantendo audit e ispezioni periodiche. La Funzione Internal Audit deve verificare che i contratti includano clausole di accesso, ispezione e audit, assicurando la cooperazione del fornitore e la possibilità di monitorarne la performance in modo continuativo.

È quindi essenziale che i contratti con i fornitori proteggano gli interessi dell'organizzazione, prevedano meccanismi di gestione delle relazioni e stabiliscano una revisione periodica delle performance, in linea con i requisiti di sicurezza e resilienza operativa imposti dalla normativa.

Un nuovo set di competenze per la Crypto Era

Il panorama crypto si evolve a una velocità vertiginosa. Per affrontare le sfide emergenti, le Funzioni Internal Audit devono sviluppare competenze tecniche avanzate e adottare strumenti innovativi.

La formazione continua e la padronanza di tecnologie chiave – tra cui blockchain, crittografia, data analytics, ICT, cybersecurity e normative crypto, anche cross-border – sono essenziali. Allo stesso modo, è imprescindibile l'utilizzo di strumenti avanzati di data analytics, soluzioni di blockchain monitoring (sia open source che proprietarie) e intelligenza artificiale per migliorare l'efficacia delle analisi.

Per le Funzioni Internal Audit, restare al passo significa investire nell'apprendimento continuo e collaborare con esperti indipendenti specializzati nel settore, al fine di assicurare a tutti gli stakeholder interessati un approccio sempre aggiornato e conforme alle evoluzioni normative e tecnologiche.

[7] *Il riferimento è ad esempio ai provider di blockchain monitoring & investigation, market surveillance, Travel Rule compliance*

Conclusioni

Il settore crypto presenta sfide uniche, ma offre anche opportunità straordinarie sia per le banche tradizionali sia per i CASP.

Adottando un approccio olistico alla gestione del rischio, le Funzioni Internal Audit possono garantire che le organizzazioni affrontino con successo le sfide emergenti, proponendo soluzioni innovative e all'avanguardia.

Solo attraverso l'integrazione di tecnologie avanzate, competenze adeguate e un approccio proattivo alla gestione del rischio, le Funzioni Internal Audit potranno non solo rafforzare la sicurezza delle organizzazioni, ma anche contribuire attivamente alla loro crescita e innovazione nel nuovo panorama finanziario digitale.

Cosa può fare Protiviti

In qualità di market leader nel settore finanziario a livello italiano e globale, grazie all'esperienza acquisita tramite progetti con i più importanti attori del mercato e le competenze dei suoi professionisti, Protiviti ha definito un framework metodologico di governance e controlli mirato a supportare i Clienti nella transizione digitale e integrazione verso i servizi crypto.

Tra i principali servizi ricordiamo:

- accompagnamento nella conoscenza, interpretazione e analisi di applicabilità dei requisiti regolamentari
- on-chain, off-chain e Osint investigation
- crypto-asset due diligence
- assessment sulla gestione e custodia delle chiavi private
- assessment della Proof of reserves
- cybersecurity e ICT audit
- analisi di bilanciamento tra le possibilità offerte dalla blockchain e i dettami del GDPR
- ESG assessment
- Third parties due diligence

CONTATTI

Francesco Monini
Managing Director
francesco.monini@protiviti.it

Riccardo Confalonieri
Associate Director
riccardo.confalonieri@protiviti.it

Mattia Santi
Manager
mattia.santi@protiviti.it