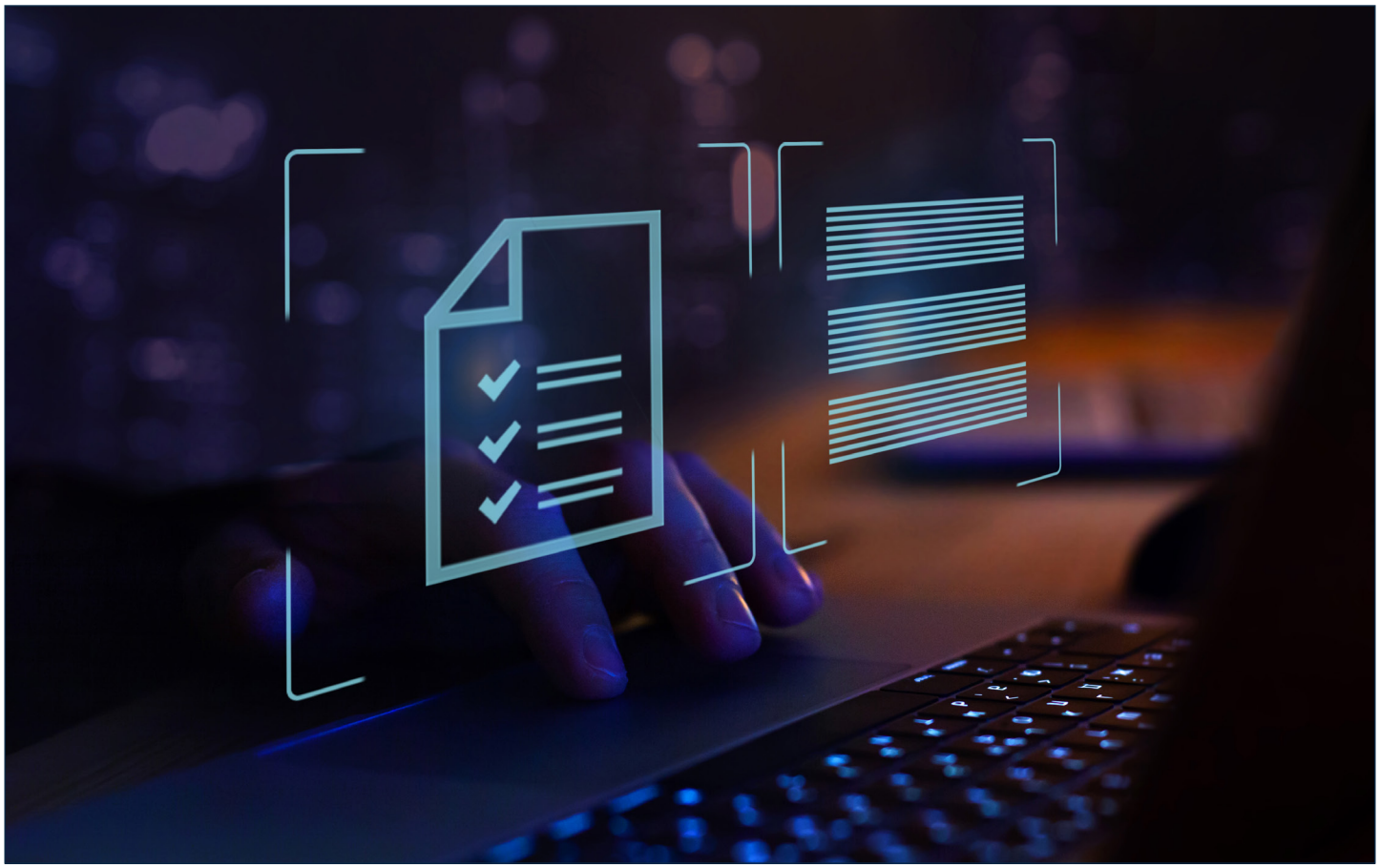
Risk Resources

# Digital asset and crypto compliance

## New risks and regulatory expectations

Risk.net April 2026

White paper



Insider information, personal trading and the conflict controls firms need now

Risk.net

MCO MyComplianceOffice

## Contents

2 Introduction

3 The new regulatory reality for digital assets

4 Why employee conduct is the missing layer

5 The emerging risk profile of employee crypto activity

6 Readiness differs by firm type – but not by control standard

7 The case for a unified, cross-asset framework

8 Practical priorities for compliance leaders

9 Looking ahead

## What a practical control architecture looks like

MCO's (MyComplianceOffice's) Digital Asset Personal Trading capability is part of its broader Know Your Employee suite, and is designed to extend employee trading oversight into digital assets without splitting the control environment by asset class.

Today, next-generation technology enables capabilities such as:

- Pre-clearance across a broad range of digital assets
- Native wallet recognition
- Conflict checks through configurable rules
- Exchange and wallet integrations
- Digital asset holdings tracking
- Audit-ready reporting
- Digital asset transaction capture, including tokenised securities, such as MSFTx.

Combined with Personal Trading Manager, MCO provides a single platform for employee trading and conflict monitoring across traditional securities and digital assets. It equips firms with digital asset readiness, which is not only about building a crypto-only sidecar but more about extending conduct, conflict and governance controls across a converging market structure.

Learn more

Cover image: Anyaberkut/Getty

Published by Infopro Digital

# Introduction

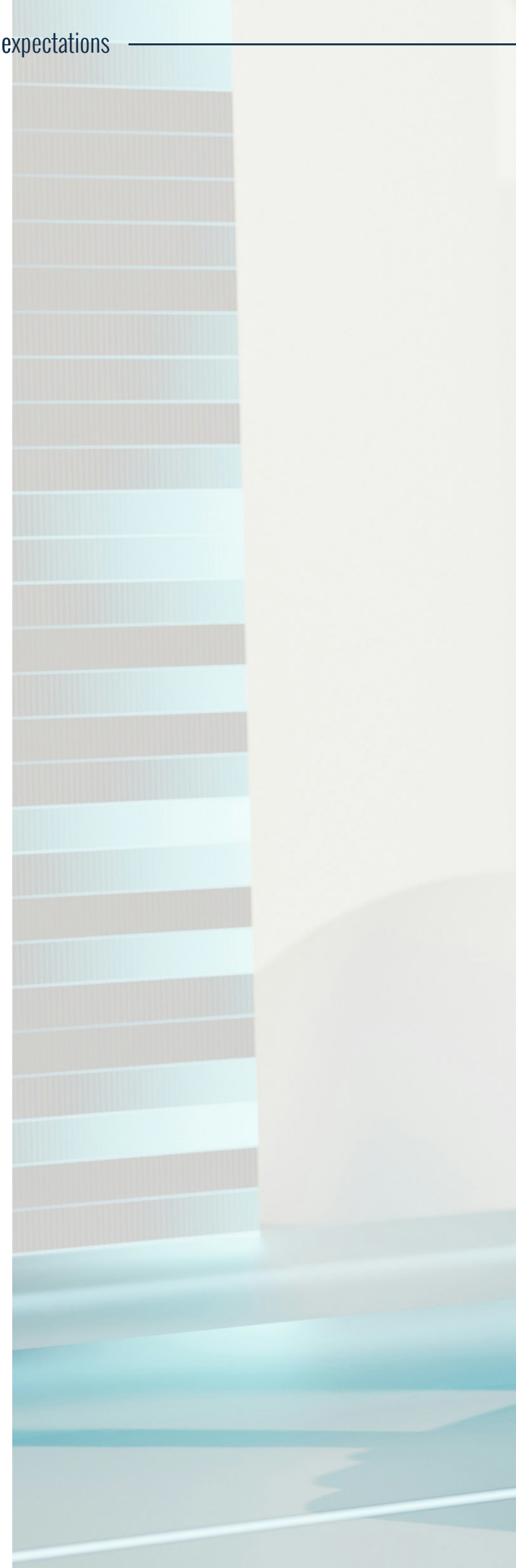
Digital assets are no longer a side market for regulated finance. That argument is over. Spot bitcoin exchange-traded products in the US, the implementation of the European Union's Markets in Crypto-Assets Regulation, Hong Kong's virtual asset licensing regime and Singapore's tightening approach to digital token service providers all point in the same direction: digital asset activity is moving into the regulated core of financial markets, from beginning to end, not orbiting around it.

For compliance leaders, however, the more important shift is not simply that digital assets are being regulated; it is that regulators, boards and firms are starting to look past the asset itself and focus instead on conduct – who is holding, who is trading, what conflicts exist, where information sits, how employee activity is monitored and whether governance has kept pace with market structure. That is a more difficult question for many institutions because it exposes a gap that has been easy to ignore. Most firms have mature controls for securities personal trading. Far fewer have an equivalent framework for employee digital asset activity across wallets, exchanges, decentralised finance (DeFi) venues, staking arrangements and digital asset-related outside business activities.

That gap matters now because the market itself has changed: institutional adoption has deepened, traditional firms are exploring custody, tokenisation and distribution models, crypto-native firms have spent the past several years building more formal risk and control environments, and the old defence that digital assets were peripheral, speculative or operationally separate from mainstream finance is no longer credible. As one senior market surveillance executive at a major crypto platform put it: "Crypto isn't a flash in the pan that's going away anytime soon."

US regulators, including the Office of the Comptroller of the Currency (OCC) and the US Securities and Exchange Commission (SEC), are publicly stating that tokenised mutual funds must be treated like their real-world asset counterparts.

As digital assets and traditional financial instruments converge, employee conduct becomes the missing control layer. Firms that close that gap early will do more than reduce regulatory risk. They will build a cleaner operating model for a market structure that is becoming more cross-asset, more data-intensive and more difficult to supervise through siloed controls.



# The new regulatory reality for digital assets

The regulatory backdrop remains uneven, but the direction is increasingly consistent. Europe has moved the market from prolonged anticipation to an operating regime with real compliance obligations. Hong Kong has imposed a formal licensing structure for virtual asset trading platforms. Singapore has continued tightening expectations around digital token service providers. The US remains contested in places, but the direction of travel is plainly towards more formalised oversight, clearer categorisation and greater market accountability. The SEC and the Commodity Futures Trading Commission are staking out their coverage responsibilities, and the OCC has taken a position on tokenised securities.

What matters is not perfect harmonisation – it is convergence around supervisory logic. Michael Versace, research director at Chartis Research, says: “Regulators are converging on themes of ‘same risk, same rules’, enhanced transparency of personal holdings and tighter management of conflicts in high-volatility or illiquid digital assets.”

That is a useful way to understand the moment. The regulatory perimeter may still vary by jurisdiction, but the conduct logic is becoming more recognisable.

John Kearney, product director at MCO (MyComplianceOffice), says regulators are moving past taxonomy. The question is no longer simply whether an asset is labelled a security or a token, but whether firms can identify, manage and control the underlying risks to market integrity and conflicts of interest.”

John Kearney, MCO

That matters because digital assets now touch several control domains at once. Personal trading is one of these domains, outside business activities are another and insider information handling is a third. Tokenised assets make these overlaps more acute by blurring the old boundary between traditional and digital instruments. Once a firm has both types of activity in motion — or even employees participating in them personally — the distinction becomes less useful from a control perspective.

This is why the debate has moved beyond product regulation. Compliance teams are being pushed towards a harder question: can the firm apply equivalent standards of disclosure, pre-clearance, monitoring, escalation and evidencing across securities and digital assets? In many cases, the answer is still no.

# Why employee conduct is the missing layer

The weakness in many firms' current approach is structural. Traditional employee personal trading frameworks assume intermediated markets, identifiable brokerage accounts, standardised confirmations and reasonably stable channels for data capture. Digital assets disrupt each of those assumptions.

A firm may know where an employee's brokerage account sits. It may receive feeds, statements or duplicate confirmations. It may have a tested reconciliation process. But, as Kearney notes, with DeFi, "the firms don't have a very good visibility into where that's held", whether across offshore exchanges, self-custody wallets or other structures that many compliance teams still do not fully understand.

The anonymous or pseudo-anonymous features of crypto add another complication. The senior market surveillance executive says that an employee may tell the firm about some wallets and fail to disclose others. Without strong analytics or reliable reporting arrangements, the firm may never know.

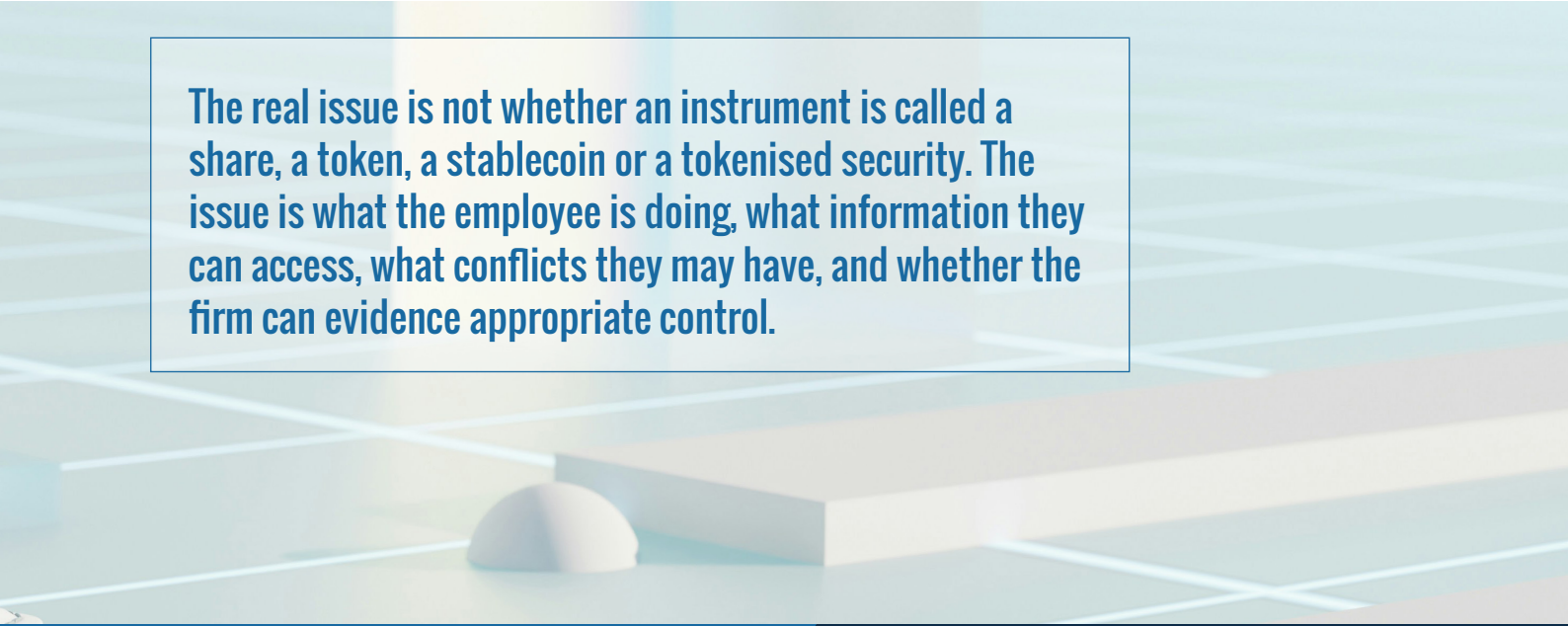
This is where many firms make the wrong move. They try to extend a securities-era framework with light cosmetic edits, adding a handful of large tokens to a restricted list and assuming the problem is covered. It is not. "Chartis recommends that firms move from product-by-product rules to a holistic framework that maps risks by activity type (for example, holding, trading, lending, advice) regardless of instrument label," says Versace.

The real issue is not whether an instrument is called a share, a token, a stablecoin or a tokenised security. The issue is what the employee is doing, what information they can access, what conflicts they may have and whether the firm can evidence appropriate control.

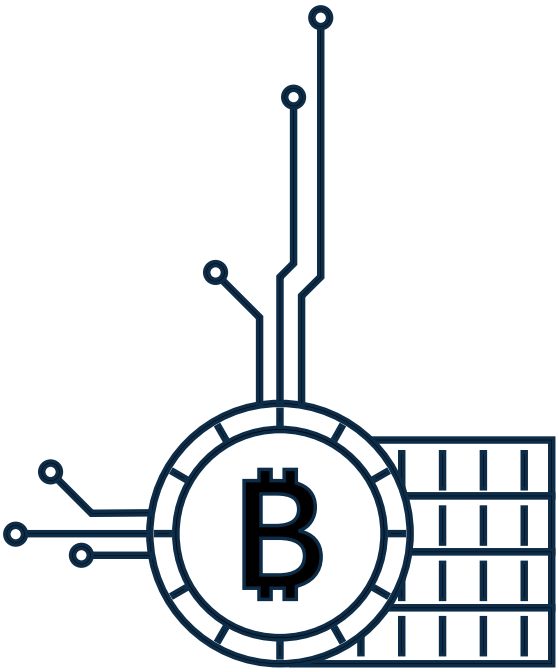
Majda Skrijelj, senior compliance officer in the Office of the Chief Compliance Officer at the Council of Europe Development Bank (CEB), points to another important problem. In tokenisation initiatives, the number of insiders can quietly expand. External advisers, technical specialists, consultants and other third parties may all gain advance visibility into projects and transactions. Policies designed for a narrower insider population can miss that expansion unless they are deliberately rescoped.

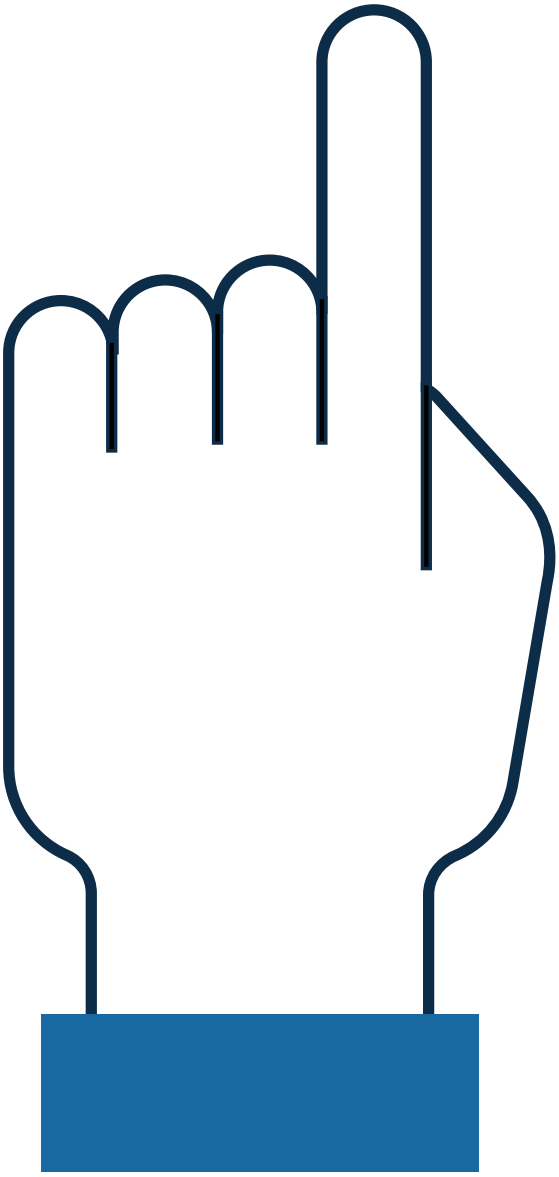
The result is not just a coverage problem, it is an evidencing problem. A firm may have policies on paper but will still struggle to prove that it can identify holdings, trace activity, connect that activity to an employee and run meaningful checks against conflicts or material non-public information. That is where regulatory reviews become uncomfortable.

The real issue is not whether an instrument is called a share, a token, a stablecoin or a tokenised security. The issue is what the employee is doing, what information they can access, what conflicts they may have, and whether the firm can evidence appropriate control.



# The emerging risk profile of employee crypto activity





The first and most obvious risk is personal trading. The issue is not that digital assets invented personal trading risk; it is that they changed its shape as well as the control structures for personal trading. Markets are continuous, venues are fragmented and data is often incomplete or dispersed. Employees may access crypto exposure through centralised exchanges, self-hosted wallets, token launches, staking arrangements or governance participation. The surveillance challenge is wider, faster and less standardised than in listed securities.

The second is insider risk. In traditional markets, firms at least operate within relatively familiar information regimes. In digital assets, information can move through token listings, protocol governance, private communities, technical advisers, online networks and informal relationships 24/7 before it appears in formal market channels. The senior market surveillance executive calls insider information “the biggest risk because it’s the hardest to identify right now in crypto”.

The third risk is outside business activity. This area is easy to underestimate because it does not always resemble a conventional conflict at first glance. An employee advising a protocol, validating on a blockchain, holding a governance token or promoting a project online may not think of that activity as equivalent to a directorship or securities-related side role. Compliance teams should. CEB’s Skrijelj provided a simple, but telling, example: an employee who advises a DeFi protocol while also holding or validating the same token is plainly sitting inside a conflict structure, particularly if the role is undisclosed.

The fourth risk is beneficial ownership and control. Many institutions still think in account-based terms. But digital assets force a move towards activity-based surveillance. Who controls the wallet? Who benefits from the position? Who is directing the bot? MCO’s Kearney notes that artificial intelligence and automated trading are likely to increase the amount of monitoring firms will need to do. Once bots begin trading on behalf of employees across digital venues, the reporting and control burden rises again.

None of these are fringe scenarios. They are the predictable by-products of a market structure built for portability, pseudonymity and disintermediation.

# Readiness differs by firm type – but not by control standard

Crypto-native firms and traditional regulated firms are starting from different places.

Crypto-native firms often understand the technology and market structure better. Their challenge is different: building institutional-grade governance around fast-moving businesses and employee populations that may have grown up in a less formal conduct culture. As the senior market surveillance executive at a major crypto platform noted, employee buy-in and education remain central. Staff need to understand that abusive or manipulative trading in crypto is not somehow exempt from the same consequences that would apply in traditional markets.

Traditional firms face the opposite problem. They usually have mature governance, but the architecture was built for brokerage accounts, not wallets; for intermediated markets, not DeFi; and for well-defined covered securities, not a proliferating universe of tokens, tokenised instruments and adjacent roles. Versace argues that firms need to move away from product-by-product rules and towards a framework that maps risks by activity type, regardless of instrument label.

Still, both types of firms are heading towards the same destination. The control standards are converging even if the paths differ. Firms need to know what employees hold, where they trade, what outside roles they perform, what information they can access and whether those activities create unmanagable conflicts.

# The case for a unified, cross-asset framework

Separate systems may feel manageable in the short term, but they create grey areas, duplicate work and blind spots between asset classes. This is where the case for a unified framework becomes strongest.

MCO's Kearney puts it plainly: when conflicts are managed on different systems, "there is a big opportunity for things to slip through the cracks". CEB's Skrijelj says that, from a regulator-facing angle, a unified framework "closes the arbitrage gap".

If securities and crypto sit in separate systems, an employee who is determined can structure activity to stay below the radar.

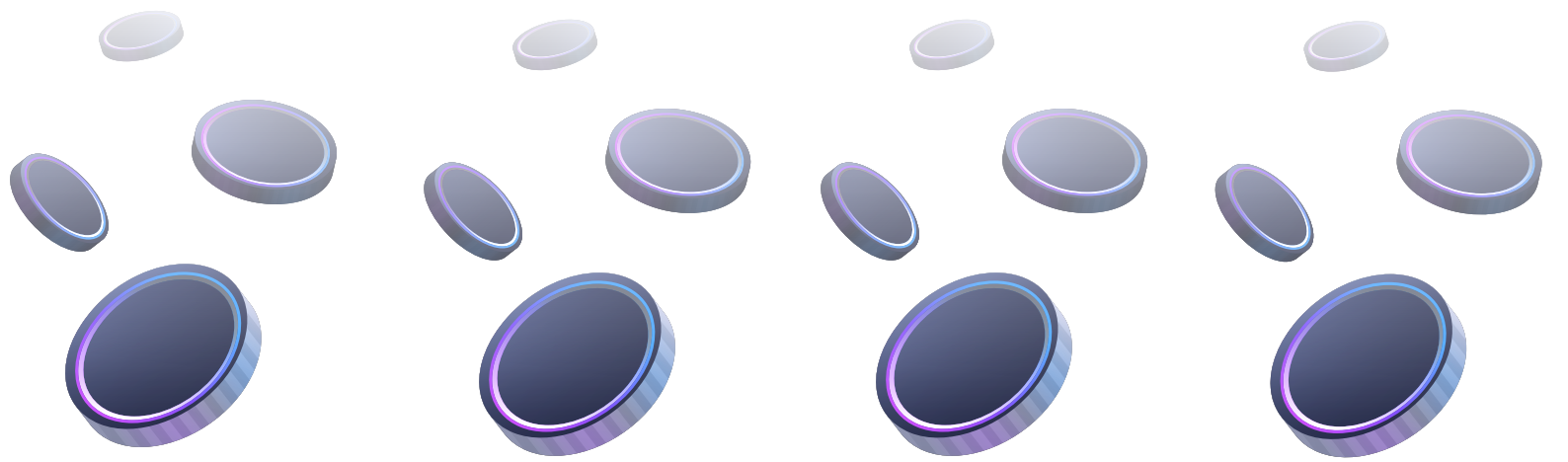
"The real insider risk arises when issuer restrictions apply in one channel but not another," says Kearney. "An employee who is wall-crossed on Microsoft may be prevented from trading Microsoft Corporation (MSFT) conventional personal account dealing controls, while still gaining equivalent economic exposure through tokenised MSFT (MSFTx) on Kraken in an account outside the firm's normal monitoring framework. Where securities and digital assets are governed in separate systems, the firm risks missing a control failure that is economically obvious even if operationally fragmented."

Chartis' Versace says that, from an operational and risk perspective: "A single cross-asset framework lets firms apply consistent definitions of covered activity, conflicts and escalation paths, reducing grey areas that employees can exploit." That is the real value. A unified framework is not a technology talking point. It is a way to reduce interpretive ambiguity and tighten the control perimeter.

This does not mean treating every instrument identically. Skrijelj warns that firms should not assume crypto assets and traditional financial assets are operationally identical. They are not. But she is equally clear that insider trading in a digital asset should carry "the same gravity" as insider trading of a traditional asset. The point of a unified framework, therefore, is not sameness for its own sake. It is consistency of control logic wherein common definitions of covered activity, common escalation standards, common evidencing and a single view of employee conduct risk across asset types.

That has immediate operational benefits: it reduces duplication; it makes data integration and reporting more coherent; it improves surveillance for patterns that span equities, tokens, derivatives and side activities; and it produces a better exam narrative – one framework, one audit trail and one governance model.

There is, however, an important caveat. A platform is only as good as the data it receives. Skrijelj says if employees do not disclose non-custodial wallets, DeFi positions or outside activities, "the platform will remain blind". Today, technology can narrow the gap and capture digital wallet activity, but culture, training and policy scope still matter.



# Practical priorities for compliance leaders

For the next few years, the sensible agenda is not maximalist – it is disciplined.

First, define scope properly. Firms should be explicit about which digital assets, venues, wallets, activities and roles are in-scope, what is prohibited, what requires pre-clearance and what must be disclosed. Policy ambiguity remains one of the biggest self-inflicted problems in this area. Versace at Chartis recommends that firms first clarify policy scope by explicitly defining which digital assets, venues and roles are in-bounds or prohibited, then embed those definitions into training and attestations.

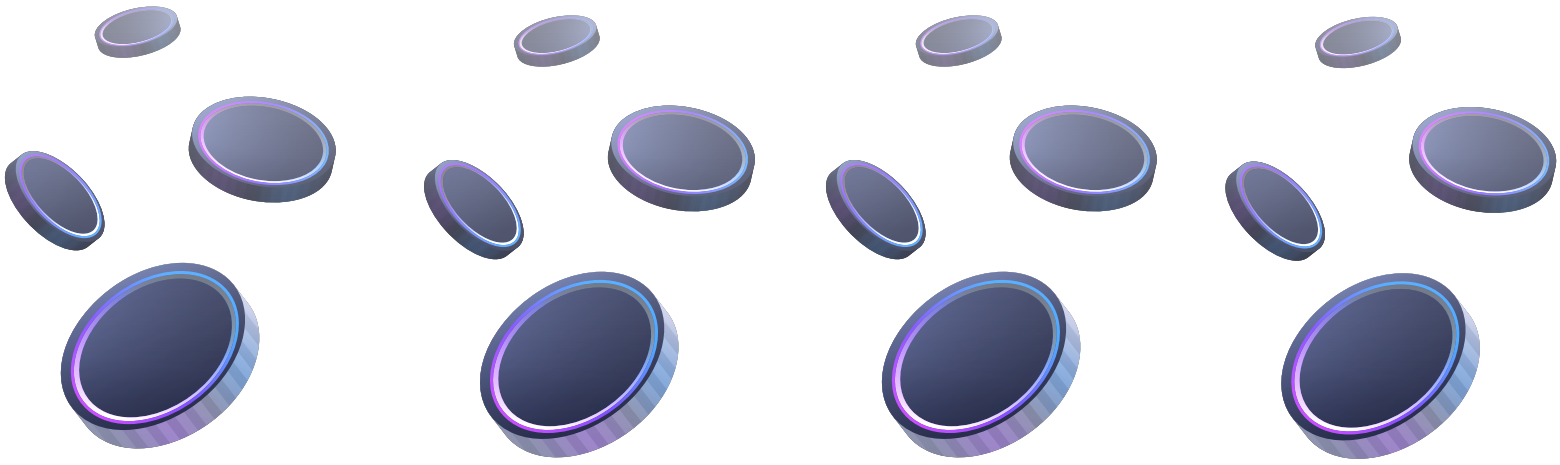
Second, identify where employee activity actually takes place. The emerging market of digital asset risk analytics (for example, Metrika, Lukka, Particula) requires chief compliance officers to better understand the data/analytics available from these firms to better monitor employee activities in digital markets.

Kearney's recommendation is that firms determine which employees have digital asset accounts and what they are trading. Firms cannot supervise what they have not inventoried.

Third, improve data capture and reconciliation. That means moving beyond attestation-only models where possible and establishing mechanisms to capture activity across major exchanges and wallets, with enough auditability to withstand review. The operational market is beginning to move this way, with emphasis on wallet recognition, exchange and wallet integrations, conflict checks and audit-ready reporting.

Fourth, rescope conflict frameworks to include digital-asset outside-business activities, token-related advisory roles, governance participation and broader insider populations around tokenisation initiatives. This remains too narrow in many firms.

Fifth, prepare for evidencing, not just policy drafting. Examiners will not stop at asking whether the firm has a digital asset policy – they will want to know if it works.

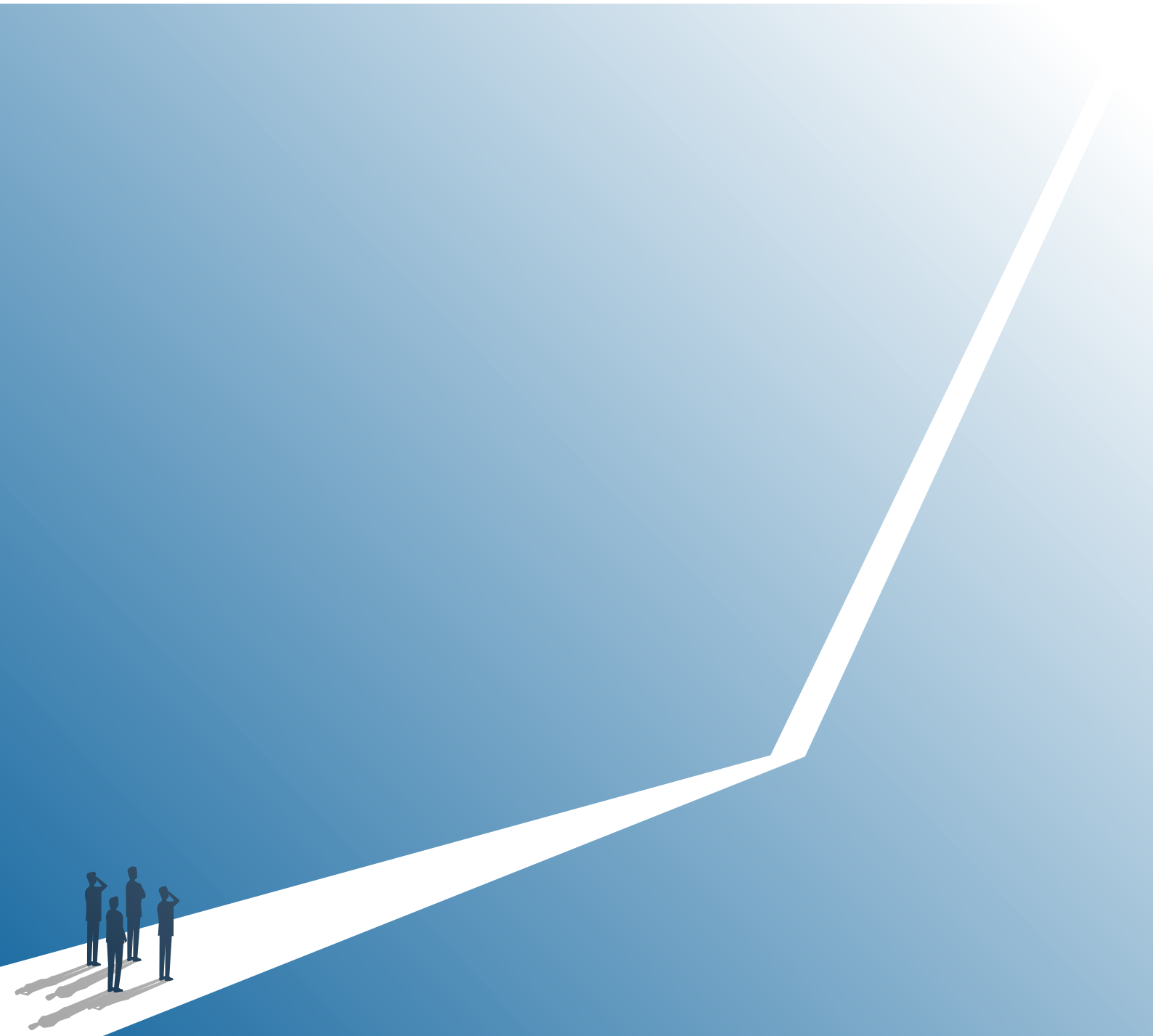


# Looking ahead

The strategic question for compliance leaders is no longer whether digital assets will matter. It is whether the firm's control model is built for a market in which digital and traditional assets increasingly coexist, overlap and, in some cases, become interchangeable from a conduct risk perspective.

The firms that handle this well will not be the ones with the thickest policy documents. Instead, they will be the ones that move early to unify surveillance logic, close disclosure gaps, expand conflict definitions and create evidence that stands up under scrutiny.

Digital assets may have arrived through a different door but, for compliance, they are rapidly becoming part of the same house.




Risk.net


MCO
MyComplianceOffice