

# Interne audit in de crypto-industrie

**De Europese crypto-industrie professionaliseert in hoog tempo. Met de inwerkingtreding van MiCAR is een nieuw tijdperk aangebroken: van registratieplicht onder DNB naar een volwaardige vergunning onder toezicht van de AFM. Medio 2025 telde het laatste DNB-register nog circa 40 registraties; inmiddels hebben 22 partijen een MiCAR-vergunning verkregen. Daarmee is crypto definitief onderdeel geworden van het gereguleerde financiële stelsel. Die ontwikkeling vraagt om volwassen governance, stevig risicobeheer en onafhankelijke assurance – precies waar interne audit waarde toevoegt.**

## De Europese cryptomarkt is in beweging

De Europese cryptomarkt beweegt zich momenteel langs meerdere strategische lijnen. Een deel van de partijen kiest nadrukkelijk voor volledige MiCAR-vergunning en Europese schaal via het EU-paspoort. De toenemende regeldruk leidt tot consolidatie in de markt, maar er zijn ook crypto-organisaties die zich juist specialiseren in specifieke nicheactiviteiten. Vooral in de sfeer van stablecoins zien we ook integratie met traditionele financiële instellingen, waarbij bijvoorbeeld banken en “neo-banken” crypto-activiteiten inbedden binnen hun bestaande bedrijfsprocessen en productlijnen. Deze strategische keuzes zijn bepalend voor de eisen aan risicobeheer en interne beheersing.

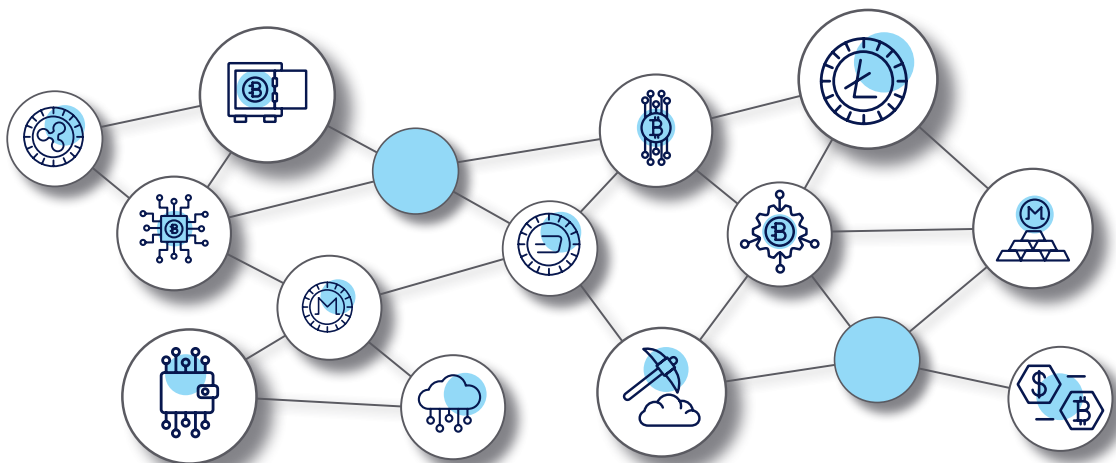
## Volwaardige financiële instellingen

Crypto-organisaties die onder MiCAR een vergunning hebben verkregen, verschillen in veel opzichten minder van ‘reguliere’ financiële instellingen dan vaak wordt gedacht. Zij opereren onder toezicht, moeten voldoen aan eisen op het gebied van governance, compliance en integere bedrijfsvoering en hebben te maken met regelgeving zoals DORA. Ook de inrichting

van AML/KYC-processen vertoont belangrijke overeenkomsten met die van betaalinstellingen en egi's (elektronisch geldinstellingen). Wanneer crypto-organisaties assets van cliënten bewaren of beheren, raken de vereisten aan principes die bekend zijn uit MiFID-regelgeving. Natuurlijk zijn er ook technologische verschillen – blockchain als onderliggende infrastructuur is fundamenteel anders – maar organisatorisch en beheersmatig bewegen deze partijen zich steeds nadrukkelijker binnen het domein van het reguliere financiële toezicht.

## Risicobeheer in een technologiedreven omgeving

De technologie waarop crypto-organisaties bouwen, brengt specifieke risico's met zich mee. De snelheid en onomkeerbaarheid van blockchaintransacties vergroten de impact van fouten of beveiligingsincidenten. Private key-beheer, smart contract-kwetsbaarheden en afhankelijkheid van externe technologiepartners vereisen een hoog niveau van IT-beheersing en monitoring. Tegelijkertijd gelden voor stablecoin-uitgevers aanvullende eisen rond het beheer van onderliggende reserves en liquiditeitsrisico's.



De combinatie van innovatieve technologie en financiële verantwoordelijkheid maakt effectief risicobeheer cruciaal. De uitdaging ligt in het integreren van technologische aspecten binnen een robuust governance-raamwerk. Dat vereist niet alleen technische expertise, maar ook een cultuur waarin risicobewustzijn en transparantie centraal staan.

### **Gedrag en cultuur als kritieke succesfactor**

Technologie en regelgeving zijn belangrijk, maar uiteindelijk wordt risicobeheer bepaald door menselijk gedrag. Mensen maken het verschil, maar waar wordt gewerkt, worden ook fouten gemaakt. Wij zien in de praktijk hoe snelgroeiende organisaties soms struikelen over hun eigen succes. Incidenten in de internationale cryptowereld laten zien wat er kan gebeuren wanneer de makkelijke oplossing wordt gekozen, wanneer kritische vragen uitblijven of wanneer te veel wordt vertrouwd op (de onfeilbaarheid van) een kleine groep sleutelfiguren. Dan is niet de regelgeving het probleem, maar het gedrag van mensen en de cultuur binnen de organisatie. Risico's zoals groei zonder voldoende tegenkracht, innovatie zonder duidelijke procedures of een cultuur waarin resultaten belangrijker zijn dan beheersing, vergroten de kwetsbaarheid van de organisatie.

Juist daarom kijken wij verder dan procedures op papier. Worden risico's écht besproken in het managementteam? Is duidelijk wie eindverantwoordelijk is voor key controls zoals AML-issues, het monitoren van uitbestede IT-diensten en hoe wordt omgegaan met spanning tussen time-to-market en security? Hoe wordt omgegaan met incidenten: defensief of lerend? En minstens zo belangrijk: ervaren medewerkers ruimte om afwijkingen of zorgen tijdig te melden?

Als interne auditors maken we deze onderwerpen concreet en toetsbaar. Wij hebben hiertoe ook expertise op het gebied van gedrag in huis. We spreken met medewerkers op verschillende niveaus, toetsen besluitvorming in de praktijk en



## MiCAR en interne audit

De MiCAR is een Europese Verordening uit 2023, genummerd (EU) 2023/1114 en heet officieel "Verordening betreffende cryptoactivamarkten".

Een belangrijke rol in de MiCAR is er voor het "Crypto Whitepaper". Dit kun je enigszins vergelijken met een prospectus voor andere financiële producten, maar bij dit document wordt geen assurance gegeven.

In de MiCAR komt het woord 'audit' (ook als 'auditverslag' of 'auditor') 25 keer voor. Veel aandacht gaat daarbij uit naar het auditverslag dat door onafhankelijke auditors wordt opgesteld. Maar waar 'audit' staat wordt veelal verwezen naar de 'statutory auditor', in de Nederlandse context veelal de externe accountant.

De indeling van de MiCAR maakt onderscheid tussen:

- Asset-Referenced Tokens (ART's)
- E-Money Tokens (EMT's)
- Crypto-Asset Service Providers (CASPs)

Eisen aan de governance worden gedefinieerd in artikel 34 (ART's), artikel 43 (EMT's) en artikel 63 (CASPs). Gemeenschappelijke eisen zijn onder meer:

- Een solide governance structuur (incl. eisen aan bestuurders)
- Effectief risicobeheer (waaronder ook DORA)
- Interne controlemechanismen

Het bestuur kan de uitvoering delegeren, maar niet de verantwoordelijkheid voor de effectiviteit van het risicobeheer: "Het leidinggevende orgaan [...] beoordeelt, en toetst periodiek, de effectiviteit [...], en neemt passende maatregelen om eventuele tekortkomingen [...] weg te werken."

leggen bloot waar formele governance en feitelijk gedrag uiteenlopen. Niet om als politieman corrigerend op te treden, maar wel om signalen te vertalen naar observaties en mogelijke verbeteringen. Zo dragen wij actief bij aan een professionele cultuur waarin transparantie, aanspreekbaarheid en risicobewustzijn vanzelfsprekend zijn – en waarin innovatie en beheersing elkaar duurzaam versterken.

### Interne audit als strategische sparringspartner

Voor bestuurders in de crypto-industrie biedt interne audit onafhankelijke en objectieve assurance over de effectiviteit van governance, risicobeheer en interne beheersing. Op basis van een gestructureerde risicoanalyse toetst interne audit of processen daadwerkelijk functioneren zoals bedoeld en of beheersmaatregelen effectief zijn ingericht. Daarbij wordt gewerkt volgens internationale professionele standaarden en met een systematische, evidence-based aanpak. De interne auditor hanteert consequent twee centrale vragen: “Is dat zo?” en “Waar blijkt dat uit?”

Voor bestuurders en toezichthouders betekent dit dat zij niet uitsluitend hoeven te vertrouwen op managementinformatie, maar beschikken over een onafhankelijke beoordeling van de beheersing van kritieke risico's – van AML-compliance, IT-security tot en met eventueel vragen

over de cultuur van de organisatie. Door het uitvoeren van interne audits verkleint het bestuur de kans op onaangename verrassingen. Dat draagt ook bij aan vertrouwen van stakeholders, klanten en toezichthouders en is daarmee van toegevoegde waarde voor de organisatie.

### InAudit is er om u te helpen!

Voor veel crypto-organisaties is de interne auditfunctie niet de eerste prioriteit. InAudit kan u daarom helpen om deze zorg over te nemen door flexibel in te spelen op de fase waarin uw organisatie zich bevindt. Wij kunnen de interne auditfunctie onafhankelijk en professioneel uitvoeren, maar ook ondersteunen bij het versterken van risicomanagement, governance en IT-security. Desgewenst nemen wij (tijdelijk) de CISO-functie op ons of vullen deze aan met specifieke expertise. Met onze achtergrond in de financiële sector en onze betrokkenheid bij de ontwikkelingen rond MiCAR begrijpen wij de context waarin u opereert. Samen zorgen we ervoor dat innovatie hand in hand gaat met beheersing. Wij zijn er om u te helpen. ◆



## Interne audit in de crypto-industrie

