AML RIGHTSOURCE

Digital Asset Compliance Series
Issuance 3 of 7

KYB & Beneficial Ownership Standards for Institutional Clients

Corporate Customer Due Diligence in Digital Asset Firms
AML & Sanctions Practices in the Digital Asset Industry

Know Your Business (KYB) - Corporate Customer Due Diligence

KYB is the process of verifying the identity and legitimacy of corporate or institutional customers (business accounts). Whenever a crypto exchange or financial institution onboards a legal entity (company, partnership, trust, etc.) rather than a natural person, it must perform KYB due diligence in addition to KYC for that entity's principals. KYB typically involves collecting the business's official registration documents, understanding its ownership structure, and identifying the Ultimate Beneficial Owners (UBOs) - usually persons owning above a certain threshold (e.g. >25%) of the company - and then verifying those individuals' identities as well. KYB also entails assessing the nature of the business (what it does, expected account activity) and checking the entity and its owners/directors against sanctions or high-risk lists.

Here's how KYB controls are implemented across the industry:

KYB in Centralized Exchanges and Custodians

Leading exchanges offer corporate or institutional accounts that require KYB onboarding. For example, Kraken, Coinbase, Binance, and others have separate sign-up flows for businesses. The exchange will ask for documents such as: proof of incorporation (e.g., articles of incorporation or business registration extract), proof of the business address, board resolution or authorization for the account, and identification information for directors and major shareholders/UBOs. An organizational chart or ownership structure may be requested if the company has parent or subsidiary layers, to ensure the exchange can see through any shell companies to the ultimate owners. Each UBO (often defined as owning >25% shares, though some jurisdictions use >10%) must undergo personal KYC (provide ID, etc.) just like any retail customer. The exchange's compliance team will verify the company's registration via government databases or third-party business registries.

Many use KYB service providers or APIs (such as Trulioo's Global Business verification, LexisNexis, or Sumsub, KYC-Chain, HyperVerge, etc.) which can auto-fetch data from official corporate registries in various countries to confirm the business is legitimate and active. They also use databases to screen the company name and registration number for any negative information (e.g., whether the company itself is sanctioned or has a known fraud history), and to perform sanctions/PEP/adverse media screening on the company's officers and UBOs. For example, if onboarding a corporate crypto treasurer or a fund, an exchange will check that none of the principals are on OFAC or other sanction lists and that the business isn't based in a prohibited jurisdiction.

Regulatory expectations for KYB are well-established: under the EU's 5th/6th AML Directives and FinCEN's CDD Rule (currently being enhanced by the new limited U.S. beneficial ownership registry), financial institutions must identify and verify the beneficial owners of legal-entity clients. Crypto CASPs under MiCA are explicitly obliged to apply full customer due diligence to corporate clients just as to individuals. In practice, exchanges often apply a risk-based approach: a small locally registered startup may undergo a simpler KYB, whereas a complex offshore trust or a client in a high-risk industry will face enhanced due diligence (e.g., providing audited financial statements, information on source of funds, etc.). KYB can be resource-intensive - challenges include inconsistent global registry data, verifying identities across jurisdictions, and detecting complex ownership chains (e.g., layered through multiple shell companies).

To streamline this, many crypto businesses automate KYB using software that extracts data from uploaded company documents and cross-checks it against databases (some compliance platforms tout automated reading of company documents in 100+ languages to expedite KYB). Still, compliance analysts typically review KYB packages manually, especially for higher-risk entities. Ongoing monitoring for corporate clients is also crucial - exchanges periodically recheck whether the client's ownership or directorship has changed, whether new negative news has emerged, or whether their transaction behavior deviates from the expected profile.

For instance, if a business customer suddenly changes ownership or starts transacting with sanctioned regions, the exchange will investigate and may request updated KYB information or even exit the relationship.

KYB in DeFi

Purely decentralized protocols generally do not have a concept of a corporate customer, since they do not "onboard" customers at all - everyone interacts pseudonymously. A business could certainly use a DeFi platform (for example, a crypto fund could trade on a DEX using the fund's wallet), but the protocol would treat them like any user: just an address. Thus, KYB is not performed by DeFi protocols themselves.

However, as institutional interest in DeFi grows, emerging permissioned DeFi pools require KYB/KYC vetting for access. The best example is Aave Arc, where only whitelisted institutions (who have been verified by a regulated entity, e.g. Fireblocks, as meeting KYC/KYB standards) can participate.

Similarly, some projects and industry consortia are exploring on-chain identity solutions where a wallet address can carry a credential proving it belongs to an entity that passed KYB off-chain. These approaches effectively create gated versions of DeFi for compliant institutions. Regulators appear supportive of such concepts for higher-risk DeFi activity. Notably, the EU in early drafts considered requiring DeFi projects to incorporate legal entities once they reached a certain scale, bringing those entities into the AML scope, but this has not yet been codified.

In summary, standard KYB is not conducted in decentralized protocols - there is no mechanism to submit a certificate of incorporation to a smart contract. The onus currently falls on institutions themselves to ensure they use DeFi in a compliant manner (some institutions only interact with DeFi through whitelisted intermediaries or under specific policies). This is a grey area, since if no intermediary is involved, a company could trade directly on a DEX without anyone verifying its identity - a situation fundamentally at odds with traditional KYB norms. This gap is on regulators' radar, and we may see new rules that require certain actors (such as DeFi aggregators or interfaces) to perform KYB if, for instance, they cater to institutional clients. Until then, KYB remains an unmet requirement in the DeFi space, except in limited permissioned contexts.

KYB for Other Blockchain Businesses

Many crypto-native financial service providers have institutional clients and therefore must do KYB. For example, crypto custodians often serve corporate clients (hedge funds, fintech firms) - these custodians (some of which have bank or trust charters, like Anchorage Digital in the U.S.) implement rigorous KYB, gathering entity documents and verifying officers, in line with banking standards.

Crypto payment gateways that sign up e-commerce merchants will perform KYB on those merchant businesses (to ensure they are legitimate and not, say, fronts for fraud). OTC trading desks and crypto brokers often transact with institutional investors and will require KYB info on those counterparties. A noteworthy point is that as large traditional institutions enter crypto (e.g. banks offering crypto services, or big investors trading crypto), they bring expectations of KYB on all sides - a bank will only do business with an exchange if the exchange can demonstrate robust KYB on its corporate customers to avoid indirect exposure to shell companies or sanctioned entities. Thus, even in jurisdictions where KYB for certain crypto activities might not yet be explicitly mandated, industry best practice is to conduct KYB for any significant B2B relationship to satisfy partner due diligence and prepare for likely future regulation.

One evolving factor is the rollout of beneficial ownership registries (like FinCEN's in the U.S., under the Corporate Transparency Act): these will eventually make it easier for financial institutions (including crypto firms) to verify the UBO information provided by corporate clients. Until then, KYB will continue to rely on the documentation and attestations provided by the customers, verified against public or commercial databases, and supplemented by risk-based scrutiny (e.g., extra checks for complex offshore companies).

KYB Technology: Tools and Vendors

For institutional onboarding, exchanges and crypto banks use KYB platforms that aggregate data from global corporate registries. KYC-Chain (the company behind SelfKey) provides tools for gathering corporate documents and verifying UBOs. LexisNexis and Refinitiv offer KYB solutions that screen companies and key personnel. Dun & Bradstreet and ComplyAdvantage databases can supply business background info and risk ratings. As noted, Sumsub offers a KYB orchestration product that combines registry checks, document OCR, and business sanction/PEP screening in a single workflow. Many larger firms integrate several sources - for example, an exchange might use an API to pull data from a government registry for basic info, and a separate provider for document authentication, and another for adverse media on the company's officers. The goal is to create a "360 view" of a corporate customer's risk before approval.

KYB Comparative Summary

The table below shows how KYB requirements apply across centralized exchanges, DeFi platforms, and other blockchain-native financial services:

Aspect	Centralized Exchanges (CEX)	DeFi & Other Services
KYC Requirement	Corporate customer due diligence is required for institutional accounts. Exchange collects registration documents, verifies business existence, and identifies Ultimate Beneficial Owners (UBOs) for KYC. Screens the company and key people against sanctions/PEPs. Uses KYB automation tools (registry checks, document OCR) to streamline onboarding. Essential under FATF standards and laws like MiCA (CASPs must do CDD on corporate clients).	Not applicable in most DeFi cases - protocols don't distinguish whether a user is a person or a company, and there's no onboarding process to submit company info. An institution can directly interact with DeFi without the protocol knowing its legal status. Only in gated DeFi environments (which are essentially CeFi/DeFi hybrids) would KYB occur off-chain to whitelist a business. Thus, standard KYB checks (registries, UBO IDs) are generally not performed by DeFi protocols. This is a recognized blind spot in the AML framework for now.
Other Crypto Financial Services	Yes, if onboarding businesses as clients or partners. For example, a crypto custody service dealing with corporate clients performs full KYB (verify incorporation, collect UBO IDs, etc.), just like a bank would. Crypto payment firms sign up merchant businesses and verify those businesses. Many use the same KYB vendors and processes as exchanges. In sectors like NFT marketplaces, corporate sellers or high-value traders might be subject to KYB in the future as regulations expand (some marketplaces have started voluntary KYB for big accounts).	Consistent theme across non-DeFi players: if handling institutional counterparties, KYB is expected. Banks entering the crypto space bring KYB standards with them, elevating the bar for crypto partners. Beneficial ownership registries under development (FinCEN's Corporate Transparency Act implementation) will improve cross-referencing of UBO claims in the coming years.