ACAMS ENTERPRISE

Proactively Managing Crypto AFC Risks

An Executive Summary

Background

Cryptoassets have evolved into a fast growing and quick moving sector with increased adoption amongst both private individuals and institutional clients. Institutions who initially maintained a hands-off approach to cryptoassets are increasingly aware that through client activities, counterparties and correspondent banking they do, in fact, have exposure to cryptoassets. In our Best Practice Guide, we set out the key considerations and controls that financial and non-bank financial institutions must consider to remain compliant and mitigate their AFC risks.

Crypto AFC risks and the need for proactive action

FIs and NBFIs adopt a wide spectrum of engagement with cryptoassets, from being cryptoasset-friendly to strictly prohibiting transfers. Against the backdrop of these differing risk appetites institutions can take a risk-based approach and define tolerances that would enable risk-based decision-making.

Determining crypto AFC risk exposure and inherent risks for new products and services

Determining direct exposure to cryptoassets is straightforward as the institution is aware of the products they directly provide that have crypto exposure. Determining indirect exposure and inherent risk involves a more deliberate approach. There are multiple considerations including but not limited to customer segment, product offering, customer risk profiles, and jurisdictions. Inherent risks in an institution's products vary significantly based on products and business segments.

Mitigating controls against crypto AFC risks – Individual customers

Most institutions tend to use cryptoasset analytic solutions that, as a minimum, include:

- The ability to perform due diligence on exchange/crypto providers, and assessments on specific coins
- Transaction Monitoring and screening capabilities
- Travel rule implementation mechanisms

Where FIs and NBFIs offer direct products and services, key considerations include e.g. customer's jurisdiction/domicile, the exchanges that customers may use, restrictions placed on third parties transfers.

Mitigating controls against crypto AFC risks – Institutional customers

Institutions that bank VASPs or have other direct exposure, EDD considerations should include:

- Business Scope – client reputation, their competence in crypto AFC, licenses, and composition of cryptoassets
- Jurisdictions – exposure to jurisdictions that do not regulate or ban cryptoassets
- Products – type, nature, and characteristics of cryptoassets
- Governance – evidence of robust governance in client institutions
- Sanctions – sanctions compliance program and its effectiveness

Future proofing AFC controls – Challenges and opportunities

The world of AFC is forever changing, however, the scale and pace of change in the crypto world is far greater. Best practices to manage crypto AFC risks include:

- Horizon Scanning and threat assessment
- Education
- Designing integrated AFC control ecosystems

Identifying the exposure, building a clear risk appetite statement and implementing crypto AFC controls in line with risk appetite will allow institutions to remain safe and compliant, irrespective of their stance on the future of cryptoassets.

Find Out More

Our full Best Practice Guide: Proactively Managing Crypto AFC Risks is available to ACAMS Enterprise members. Download your copy **here**.

You can find out more about ACAMS Enterprise membership by visiting our **Enterprise homepage**.

V05102022