Due diligence specifics

Dr Alexander Ressos, TEP
Of Counsel, KGP Legal LLC
Attorney-at-Law (Switzerland and Germany), Solicitor (England & Wales and Hong Kong)

Due diligence on a digital-asset business adds a layer to the ordinary legal, financial and tax review. The additional items are these.

- Customer assets. The buyer needs a reconciliation, as at a date close to signing, of the tokens the target holds for customers against the balances it owes them, on each chain, with on-chain proof of the holdings. A shortfall is the single most dangerous finding in any crypto acquisition and has been the undoing of several buyers who did not look.
- Key management. Who holds the keys to the customer wallets and the treasury, under what procedures, with what backup and with what change-of-personnel protocol. A target whose keys are held by a founder who is leaving is a target whose assets are at risk on completion.
- Regulatory history. Every FINMA or MAS enquiry, inspection, finding and undertaking, and every SRO audit report. Both regulators keep files that the buyer cannot see, so the seller's representations must be backed by documents.
- AML file quality. A sample review of customer files against the applicable standard (SRO regulations in Switzerland, PSN02 in Singapore), with particular attention to source-of-wealth documentation for the largest customers and to the travel-rule implementation.
- Hacks and incidents. Every security incident, its cause, the loss, the customer compensation and the regulatory notification. An undisclosed incident is a breach of the target's regulatory duties and a liability the buyer inherits.
- Token holdings and treasury. The target's own tokens, including any native token it has issued, with the legal classification, the lock-ups, the market-making agreements and the tax basis.
- Smart contract and code. For a target that operates protocols or smart contracts, the audit reports, the upgrade keys and the admin rights, and who holds them.
- Tax. The characterisation of the target's token transactions in each year, the VAT or GST treatment, the transfer-pricing documentation for intra-group flows and the exposure to reclassification of private gains as trading income in the founders' hands if they are selling.

Checklist

A buyer's first request list for a licensed digital-asset target in either hub should include: - the licence, the SRO or MAS correspondence file and every regulatory finding since licensing - the customer asset reconciliation at the last month end with on-chain evidence - the key-management policy, the list of key holders and the incident log - the AML policy, the last independent AML audit and a sample of

Copyright © 2026 Dr Alexander Ressos, TEP – Of Counsel, KGP Legal LLC. SingaporeIQ is an information website and gives no legal advice. For Singapore law advice through KGP Legal LLC, please write to alexander.ressos@kgplegal.com.sg

customer files - the technology risk management framework and the last penetration test - the native-token documentation (classification opinion, lock-ups, market-making agreements, treasury policy) - the three most recent audited accounts and the auditor's management letters - the transfer-pricing documentation and tax rulings - the employment and token-plan documents for key personnel - the insurance policies and claims history

Copyright © 2026 Dr Alexander Ressos, TEP – Of Counsel, KGP Legal LLC. SingaporeIQ is an information website and gives no legal advice. For Singapore law advice through KGP Legal LLC, please write to alexander.ressos@kgplegal.com.sg