Innovation & Business Exercise, IB5, SOLUTIONS

Institutional Crypto, Red-Team the Custodian

Digital Finance, BSc Course — Prof. Dr. Joerg Osterrieder

Facilitator key | every claim is fine once it survives the right question

---

How to use this key. The skill is turning a vague claim into a falsifiable question. Reward specificity: "insured by whom, for how much, with what exclusions?" beats "is it really insured?".

Claim	Exposing question	Verdict
Bank-grade security	Which standard, exactly, SOC 2 Type II? When was the last independent penetration test?	Red flag if unnamed
Fully insured	Insured by whom, what limit vs our AUM, and what is *excluded* (insider theft, hot-wallet only, per-incident cap)?	Red flag (limit usually $\ll$ AUM)
Regulated	Regulated by whom and *for what activity*? A money-transmitter licence is not a qualified-custodian charter.	Red flag if conflated
Segregated	Legally bankruptcy-remote? Segregated on-chain addresses with proof, or commingled omnibus?	Verifiable with evidence
Multi-sig cold storage	What quorum (m-of-n), who holds keys, geographic distribution, and the recovery process if a signer is lost or compromised?	Verifiable with a key policy

Must-have controls. (1) Qualified-custodian status *for the relevant activity*; (2) current SOC 2 Type II + independent audit; (3) proof of reserves and **bankruptcy-remote** segregation; (4) insurance with disclosed limits and exclusions; plus a documented m-of-n key ceremony with geographic key distribution.

The point. For an institution the product *is* trust infrastructure. "Fully insured" and "regulated" are the two claims most often technically true and practically misleading, the insurance limit and the *scope* of the licence are where allocations are won or lost.