— BRIEFING / 004 · JULY 2026

THE QUESTIONS YOUR CUSTODIAN HAS NOT BEEN ASKED.

Every custody vendor you are evaluating has answered hundreds of due diligence questionnaires. That is the problem. The standard DDQ has become a genre, and the answers have become a product. This briefing covers what those questionnaires actually test, what they systematically miss, and eight questions from the ERS custody due diligence instrument.

EXECUTIVE RISK SERVICES

Prepared for worst-case scenarios. So you don't have to.

info@executiveriskservices.com · referral or invite only

— 01 / THE PAPERWORK

WHAT THE STANDARD QUESTIONNAIRE ACTUALLY TESTS

The typical custody DDQ runs one to three hundred questions across certifications, insurance, key generation ceremonies, penetration testing cadence, and business continuity. Vendors answer it with a document library: the SOC 2 report, the ISO certificate, the insurance binder, the whitepaper. A diligence team checks the documents against the questions and produces a memo.

What this process measures is the vendor's ability to produce documentation. That is not nothing. A vendor that cannot produce clean paperwork has told you something important. But paperwork fluency and operational security are different properties, and the gap between them is where losses actually occur. The questionnaires converge on the same questions, the vendors converge on the same answers, and the exercise converges on a formality both sides complete in order to move to signature.

— 02 / THE BLIND SPOT

THE CONTROL THE PAPERWORK CANNOT SEE

Briefing 003 made the argument in full: every custody architecture, from a hardware wallet in a safe to institutional MPC with a qualified custodian, terminates in a person who can approve a transaction. Cryptography relocates that person. It never removes them.

The standard DDQ interrogates the cryptography and the corporate shell around it. It rarely interrogates the authorizer. Who are the people who can approve or co-approve movement of client assets? How were they selected, and how are they supported? What happens when one of them is coerced, compromised, or simply leaves? What does the vendor know about the physical exposure of its own signing personnel, and what has it done about it? These questions sit at the seam between cyber and physical security, which is precisely why neither the security questionnaire nor the HR policy covers them. Each discipline assumes the other has it.

— 03 / THE INSTRUMENT

WHAT A SERIOUS INSTRUMENT ASKS

A custody diligence instrument earns its keep when it produces answers the vendor has not pre-written. That means questions with three properties. They are specific enough that a marketing answer is visibly non-responsive. They probe governance and design rather than certifications, because certifications are inputs, not outcomes. And they cross the cyber-physical seam deliberately, because that is where the vendor's own blind spot usually sits.

The instrument also has to grade the answers, not just collect them. A confident answer that names a tradeoff is worth more than a flawless answer that names none. Vendors who say "we have not solved this fully, here is the compensating control" are describing reality. Vendors whose every answer terminates in an acronym are describing their document library.

— 04 / THE QUESTIONS

EIGHT QUESTIONS FROM THE ERS INSTRUMENT

A sample from the full questionnaire. Each is designed so that the quality of the answer, not the presence of one, is the signal.

01 Name every role that can individually or jointly authorize movement of client assets, including break-glass and recovery paths. Which of these roles existed in your architecture diagram, and which exist only in practice?

02 Describe the last time an authorizer left the firm. What access was retired, in what order, and how long did full retirement take?

03 What is your written protocol if an authorizer reports a threat against themselves or their family? Who is notified, and what changes about their signing authority while the threat is open?

04 Under what circumstances can a client-initiated withdrawal be slowed or stopped by a human at your firm, and who reviews that human's decision?

05 Which of your controls assume the authorizer is acting freely? What compensates when that assumption fails?

06 Describe a real incident or near miss from the last 24 months and what changed afterward. If you cannot describe one, explain how incidents reach management.

07 What does your firm know about the public discoverability of its signing personnel, and when was that last assessed?

08 If we asked to observe a signing ceremony or a recovery drill, what would we be permitted to see, and why is the rest withheld?

The full instrument, with scoring guidance and the follow-up sequences for weak answers, is available to subscribers.

ERS provides executive protection, insider-risk advisory, and custody-governance review for principals in digital assets, finance, and technology. Engagements begin with a conversation: info@executiveriskservices.com.

This briefing describes an evaluation methodology. It names no vendor, describes no specific firm's weaknesses, and contains nothing that assists an attacker; every question probes governance that a serious custodian should be able to discuss with a serious client. That restraint is the editorial policy of this series: we publish the pattern and the protective takeaway, and we omit operational detail.