

Institutional Staking | A 12-Point Vendor Checklist

By Aetsoft and Simply Staking

A practical evaluation framework for institutions assessing enterprise staking partners in 2025.

How to Use This Checklist

This checklist is intended for due diligence, vendor comparisons and internal approval workflows. Institutions can integrate these points into procurement processes, risk assessments and ongoing provider evaluations to ensure secure, compliant and scalable staking operations.

Section One: Security and Key Management

1. Key Management Architecture

- Confirm the use of secure hardware modules or multi-party computation for key generation and signing
- Ensure withdrawal keys and validator keys are separated
- Verify that private keys are never exposed in plain form
- Request documentation of key ceremonies and internal approval processes

2. Policy Controls and Access Governance

- Review role based access control and multi-person approval requirements
- Confirm segregation of duties between custody, operations and governance teams
- Check whether all staking actions follow documented and enforceable internal policies

3. Slashing Protection and Security Assurance

- Assess availability of slashing protection or insurance
- Review the provider's historical slashing record and uptime performance
- Confirm the use of redundant validators and anti double sign safeguards
- Request recent external security audits or certifications such as SOC 2 or ISO 27001

Section Two: Compliance, Legal and Reporting

4. Regulatory Alignment and Operating Framework

- Verify licensing status and jurisdictional registrations
- Review clarity of custodial roles and operational responsibilities
- Confirm the provider's understanding of evolving regulatory guidance for staking
- Ensure that contractual terms clearly define how rewards, fees and responsibilities are handled

5. KYC, AML and Sanctions Controls

- Confirm robust identity verification for all clients
- Review AML monitoring routines and sanctions screening processes
- Ensure that the provider maintains internal compliance oversight and escalation paths

6. Reporting Transparency and Audit Support

- Request complete reward and fee breakdowns
- Ensure that validator performance, reward history and transaction logs are available in exportable formats
- Confirm readiness to support external audits through structured data, attestations and documented processes

Section Three: Validator Infrastructure and Performance

7. Uptime Track Record and Reliability

- Review historical uptime and validator performance across supported networks
- Confirm multi-region redundancy and resilient failover systems
- Assess documented procedures for incident handling and rapid recovery

8. Geographic and Technical Distribution

- Verify the use of independent data centres across multiple regions
- Confirm support for multiple validator client implementations where networks allow
- Review disaster recovery plans and internal resilience testing routines

9. Blockchain Coverage and Network Flexibility

- Review the range of proof-of-stake networks supported
- Confirm the provider's ability to onboard new networks efficiently
- Ensure consistent tooling, monitoring and reporting across all chains

Section Four: Service Quality, Cost Structure and Institutional Support

10. Pricing Transparency and Fee Structure

- Review fee schedules and ensure all costs are clearly stated
- Confirm reward distribution frequency and the absence of hidden charges
- Check for minimum stake thresholds, lock periods or additional conditions

11. Support Standards and Service Level Agreements

- Confirm guaranteed response times and structured escalation procedures
- Review availability of dedicated account managers
- Assess whether 24 hour technical and operational monitoring is provided

12. Expertise, Governance Participation and Strategic Guidance

- Evaluate the provider's depth of experience across proof-of-stake networks
- Confirm participation in governance processes and awareness of protocol upgrades
- Review the ability to guide institutions through risk events, market changes and long term staking strategy