Backup And Recovery Diligence Checklist

Use this checklist to assess backup and recovery providers before you commit.

1. SCOPE AND OWNERSHIP

- Is scope explicit for servers, virtual machines, Microsoft 365, SaaS, and edge devices?
- Are exclusions documented and approved by business and technical owners?
- Is there a named owner for restore decisions during incidents?

2. RECOVERY OBJECTIVES

- Are RPO and RTO defined per critical system, not one default for all workloads?
- Do documented RPO and RTO values match the actual backup schedule and architecture?
- Are dependency maps available for applications, identity, DNS, and network paths?

3. IMMUTABILITY AND ACCESS CONTROL

- Is immutable storage enforced for required backup tiers?
- Are backup administration accounts separated from day-to-day admin accounts?
- Is there evidence that ransomware-style deletion attempts are prevented or detected?

4. RESTORE TESTING

- Are full and partial restores tested on a fixed cadence?
- Are restore test outputs retained with dates, systems, and pass or fail outcomes?
- Are failed tests turned into tracked actions with owners and due dates?

5. MICROSOFT 365 AND SAAS COVERAGE

- Is tenant-level backup in place for Exchange, OneDrive, SharePoint, and Teams?
- Are retention and legal hold requirements reflected in recovery design?
- Can the provider prove restore workflows for common user and mailbox scenarios?

6. INCIDENT AND SERVICE INTEGRATION

- Do backup and security teams use a shared incident path and evidence trail?
- Can service desk teams execute standard restore requests from current runbooks?
- Are escalation paths for severe incidents written and tested?

7. AUDIT AND PROCUREMENT READINESS

- Are RFP claims supported by dated records, not only architecture diagrams?
- Can the provider export scope, test evidence, and ownership statements quickly?
- Is there a governance cadence for reviewing backup posture and residual risk?

8. CONTINUITY AND CHANGE MANAGEMENT

- Are backup changes controlled through a formal change process?
- Are architecture and runbooks updated after every material change?
- Can a new engineer operate and recover critical systems from documentation alone?

If you want Trucell to run this checklist against your current environment, book a backup scope review from the backup and recovery page.