Audience: Procurement teams evaluating hybrid cloud, colocation, and recovery posture together.

Integrated story

Organisations suffer when cloud tenancy, network paths, identity, and backup are purchased from unrelated suppliers with no shared incident thread. Trucell scopes cloud and backup so ownership from workload to restore is explicit:

- **Private cloud and colocation** — NextDC, Equinix, and related facility patterns with remote hands and connectivity aligned to your WAN and security design.
- **Public cloud** — Azure (including AMMP where applicable), with tenancy design, landing zone expectations, and handover to managed operations when engaged.
- **Connectivity** — Business internet, fibre, and SD-WAN-style designs that affect cloud performance and failover are in the same delivery conversation when Trucell runs network services.
- **Backup and recovery** — Veeam, Datto, Microsoft 365 protection, and immutable storage strategies scoped with named RTO/RPO assumptions, restore testing, and linkage to security incident playbooks.

Governance

Change control, monitoring context, and ticket ownership connect cloud resources to the same PSA and escalation model as on-premises estates when Trucell manages both.

Evidence

Recovery tests, backup job evidence, and immutability configuration are produced for customer assurance programmes when backup services are in scope. Cross-reference the **Backup and recovery diligence checklist** and **Cloud diligence checklist** for question-level reviews.

Boundaries

Customer-owned cloud subscriptions, third-party SaaS administration, or hyperscaler contracts that exclude Trucell remain your responsibility unless explicitly transitioned under a statement of work.