Cloud and Hybrid Diligence Checklist

Use this checklist during cloud migration planning, colocation review, or managed service renewal to reduce handover risk.

1) Workload and Scope Clarity

- Confirm in-scope workloads, environments, and critical dependencies.
- Confirm which workloads stay on private or colocated infrastructure and which move to public cloud.
- Confirm business-critical recovery objectives by workload tier.

2) Identity and Access Model

- Confirm identity source of truth and administrative role boundaries.
- Confirm privileged access controls for cloud, hypervisor, and network layers.
- Confirm onboarding and offboarding controls for operators and third-party support.

3) Data Path and Residency

- Map data flow between sites, cloud regions, and backup targets.
- Confirm residency and sovereignty constraints for regulated data classes.
- Confirm encryption standards in transit and at rest across all layers.

4) Backup, DR, and Operational Proof

- Confirm backup scope across SaaS, cloud workloads, and private infrastructure.
- Confirm restore cadence, test ownership, and evidence retention requirements.
- Confirm RPO and RTO targets are measured against realistic restoration tests.

5) Network and Connectivity Readiness

- Confirm interconnect and bandwidth design for production and recovery traffic.
- Confirm failover routing and DNS ownership for critical services.
- Confirm segmentation and security controls across user, server, and management planes.

6) Run-State Ownership and Governance

- Confirm who owns day-two operations across cloud, facility, and support desk.
- Confirm escalation paths for incidents that cross provider boundaries.
- Confirm reporting cadence and artefacts for leadership, risk, or procurement review.