Internet and WAN Diligence Checklist

Use this checklist before renewing carriers, redesigning WAN, or selecting a managed connectivity partner.

1) Business-Critical Scope

- Confirm all sites, critical applications, and voice dependencies in scope.
- Confirm acceptable downtime by service (for example: voice, VPN, clinical apps, ERP).
- Confirm required failover behavior for each critical workflow.

2) Carrier and Contract Clarity

- Confirm committed SLA terms (fault response, restoration targets, notification obligations).
- Confirm what is guaranteed versus best effort in commercial terms.
- Confirm escalation ownership between carrier, MSP, and internal teams.

3) Path Diversity and Failover

- Confirm physical and logical path diversity, not only provider diversity.
- Confirm DNS, routing, and firewall behavior during failover events.
- Confirm failover tests are scheduled and evidence is retained.

4) Performance and Capacity

- Confirm bandwidth assumptions for upload-heavy and real-time services.
- Confirm latency and jitter expectations for voice and cloud workloads.
- Confirm contention and oversubscription risk for peak periods.

5) Security and Boundary Alignment

- Confirm WAN and internet design aligns with firewall and segmentation policy.
- Confirm remote access and identity controls operate consistently during failover.
- Confirm management-plane access is restricted and auditable.

6) Operational Run-State

- Confirm current network diagrams and runbooks are maintained after change.
- Confirm service desk can follow escalation and carrier engagement procedures.
- Confirm review cadence for capacity, incidents, and contract renewal risk.