Internet Failover & Redundancy Planning Checklist

Plan and verify your internet redundancy strategy with automatic failover, DNS resilience, monitoring, and incident response — 50+ items across 6 sections.

6	50+	Score	Free
PLANNING AREAS	ITEMS TO VERIFY	EACH SECTION OUT OF 10	PRINT & USE NO STRINGS

How to Use This Checklist

Complete this checklist with your network administrator or managed service provider. Test every failover mechanism rather than assuming it works. Score each section and prioritise any areas below 6 for immediate remediation.

info@cloudswitched.com
+44 2030 043 450
New London House, 6 London St, London EC3R 7LP

1 Primary Connection Health

Ensure your primary internet connection is healthy, monitored, and performing to contracted standards before planning redundancy.

- [ ] The primary connection **type, speed, and ISP** are documented with circuit reference numbers readily accessible
- [ ] A **24/7 monitoring tool** tracks uptime, latency, packet loss, and bandwidth utilisation on the primary connection
- [ ] Primary connection speeds are **regularly tested** and compared to contracted SLA minimums (test weekly as a minimum)
- [ ] The primary circuit has a **business-grade SLA** with guaranteed uptime, response times, and fault repair commitments
- [ ] The **physical path** of the primary connection into the building is documented including duct routes and termination points
- [ ] The primary **router and modem firmware** are current and on a scheduled update cycle
- [ ] Historical **uptime data** for the primary connection is retained for at least 12 months for trend analysis
- [ ] The ISP provides **proactive alerting** for circuit degradation or planned maintenance windows

Section Score: ____/10

2 Secondary Connection Setup

Your backup connection must be genuinely independent of the primary to provide real resilience.

- [ ] A secondary connection is provisioned from a **different ISP** than the primary to avoid shared infrastructure failures
- [ ] The secondary connection uses a **different technology type** (e.g., 4G/5G backup for a fibre primary, or vice versa)
- [ ] The secondary circuit enters the building via a **physically diverse route** — not the same duct, cabinet, or pole
- [ ] Secondary connection **bandwidth is sufficient** to maintain critical business operations during a primary outage
- [ ] The secondary connection has its own **dedicated router or modem** that is independently monitored
- [ ] A **SIM-based 4G/5G backup** is available as a tertiary option with adequate signal strength verified on site
- [ ] The secondary ISP's **SLA and support contacts** are documented and accessible to the IT team
- [ ] Both connections are tested for **compatibility with all critical services** (VoIP, VPN, cloud applications)

Section Score: _____/10

3 Automatic Failover Configuration

Failover must be automatic and fast. Manual intervention during an outage wastes critical minutes.

- [ ] A **dual-WAN capable firewall or router** manages both connections with automatic failover configured
- [ ] Failover triggers are configured with appropriate **health check thresholds** (ping targets, latency limits, packet loss)
- [ ] Health checks target **multiple external destinations** to avoid false failovers caused by a single target being unreachable
- [ ] Failover **switching time** has been measured and is within acceptable limits (target: under 30 seconds for most businesses)
- [ ] Active sessions (VoIP calls, VPN tunnels) are **assessed for failover behaviour** — some will drop and need to reconnect
- [ ] Load balancing between connections is configured if **active-active mode** is preferred over active-passive
- [ ] Failback to the primary connection occurs **automatically** once it is verified as stable, not immediately on restoration
- [ ] Failover **alerts are sent** to the IT team via email, SMS, or monitoring dashboard when a switchover occurs
- [ ] The firewall or router **logs all failover events** with timestamps for post-incident analysis

Section Score: _____ /10

4 DNS & Routing Resilience

DNS and routing configuration must support failover seamlessly to maintain service availability.

- [ ] DNS resolution uses **multiple upstream DNS providers** (e.g., Cloudflare 1.1.1.1 and Google 8.8.8.8) for resilience
- [ ] Internal DNS servers are configured with **forwarders to both ISP connections** to maintain resolution during failover
- [ ] Externally-hosted DNS records have **appropriate TTL values** that balance caching efficiency with failover speed
- [ ] Any services relying on **public IP addresses** have been assessed for failover — IP changes during switchover may break inbound connections
- [ ] Dynamic DNS is configured if the **secondary connection uses a different public IP** that must be updated automatically
- [ ] VPN tunnels are configured to **re-establish automatically** over the secondary connection when the primary fails
- [ ] BGP or similar routing protocols are configured if the business uses **provider-independent IP space** for seamless failover
- [ ] Mail delivery (**MX records and SPF**) has been verified to function correctly when traffic routes via the secondary connection

Section Score: _____/10

5 Testing & Monitoring

Untested failover is unreliable failover. Regular testing and continuous monitoring are essential.

- [ ] A **failover test is performed quarterly** by physically disconnecting the primary connection and verifying automatic switchover
- [ ] Failover tests include verification that **VoIP, VPN, email, and cloud services** continue to function on the backup connection
- [ ] The **time to failover** and time to failback are recorded during each test for trend analysis
- [ ] A **network monitoring system** (PRTG, Zabbix, LibreNMS, or cloud-based) continuously monitors both connections
- [ ] Monitoring alerts are configured for **high latency, packet loss, bandwidth saturation, and connection down** events
- [ ] An **external monitoring service** verifies internet availability from outside the network to catch issues invisible from within
- [ ] Monitoring alerts are configured for **high latency, packet loss, bandwidth saturation, and connection down** events
- [ ] Test results and monitoring data are **reviewed in quarterly IT review meetings** with actions tracked to completion

Section Score: ____/10

6 Incident Response Procedures

When a connection fails, clear procedures ensure fast response regardless of who is on call.

- [ ] A documented **internet outage response procedure** exists with step-by-step instructions for the IT team
- [ ] ISP **fault reporting contact numbers and procedures** are documented and accessible (not locked behind a login requiring internet)
- [ ] An **escalation matrix** defines who to contact at each stage of a prolonged outage (15 min, 1 hour, 4 hours, 8 hours)
- [ ] A **communication template** is prepared for notifying staff about internet outages and estimated restoration times
- [ ] The incident response procedure includes steps for **verifying failover has activated** and confirming critical services are running
- [ ] Contact details for the **secondary ISP's support team** are equally accessible in case both connections are affected
- [ ] A **post-incident review process** captures root cause, timeline, and improvement actions after every significant outage
- [ ] Incident response procedures are **tested annually** through tabletop exercises with the IT team

Section Score: ____ /10

7 Audit Summary & Action Plan

#	AUDIT AREA	SCORE	PRIORITY
1	Primary Connection Health	/ 10	H / M / L
2	Secondary Connection Setup	/ 10	H / M / L
3	Automatic Failover Configuration	/ 10	H / M / L
4	DNS & Routing Resilience	/ 10	H / M / L
5	Testing & Monitoring	/ 10	H / M / L
6	Incident Response Procedures	/ 10	H / M / L
TOTAL SCORE		**/ 60**	

Score Interpretation

80–100: Excellent. Your IT setup is well-managed. Focus on continuous improvement and emerging threats.
60–79: Good foundation but gaps exist. Prioritise areas scoring below 6 and create an action plan.
Below 60: Significant gaps that put your business at risk. Consider an urgent review with an IT specialist.

Top 3 Priority Actions:

1. _____
2. _____
3. _____

Additional Notes

_____

_____

_____

_____

_____

_____

Audit completed by: _____ Date: _____ Next review due: _____