CLOUDSWITCHED

FREE RESOURCE — PLANNING CHECKLIST

Internet Failover & Redundancy Planning Checklist

Plan and verify your internet redundancy strategy with automatic failover, DNS resilience, monitoring and incident response — 49 checkpoints across six planning areas. Test every failover mechanism rather than assuming it works.

6	49	/10	Fillable
PLANNING AREAS COVERED	CHECKPOINTS TO VERIFY	SCORE EACH SECTION	TICK & TYPE IN ANY VIEWER

FAILOVER · DNS RESILIENCE · MONITORING · INCIDENT RESPONSE

PREPARED FOR	PREPARED BY	VERSION	FORMAT
Cloudswitched Knowledge Library	Cloudswitched Ltd.	2026 Edition	Interactive PDF

00

How to use this checklist

Complete this checklist with your **network administrator or managed service provider**. Work through each of the six planning areas and tick every checkpoint that is **fully in place and verifiable today** — test every failover mechanism rather than assuming it works. Then award each section a score out of 10 based on how many checkpoints you can confidently tick.

A score **below 6 in any section** signals a redundancy gap that should be closed before the next outage exposes it. Use the action plan at the back to capture your top three priorities. This is an **interactive PDF** — tick the boxes and type your scores and notes directly in any modern PDF viewer.

WHAT THIS CHECKLIST IS

A practical self-assessment of your internet resilience — primary connection health, a genuinely independent secondary connection, automatic failover, DNS and routing resilience, testing and monitoring, and incident response. It is not a formal business continuity audit, but it is a fast way to surface the single points of failure that take businesses offline.

TEST, DON'T ASSUME

The most common failover failure is the one nobody tested. Physically disconnect the primary connection at least quarterly and confirm the secondary takes over within target — and that VoIP, VPN, email and cloud apps keep working on it.

The six planning areas

- **01 Primary Connection Health** — type, speed, ISP, monitoring, SLA and physical path.
- **02 Secondary Connection Setup** — different ISP, diverse route, sufficient bandwidth.
- **03 Automatic Failover Configuration** — dual-WAN, health checks, switching time, failback.
- **04 DNS & Routing Resilience** — multi-provider DNS, TTLs, VPN re-establish, MX/SPF.
- **05 Testing & Monitoring** — quarterly tests, monitoring system, external checks, reports.
- **06 Incident Response Procedures** — outage runbook, escalation matrix, comms, post-incident review.

01

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.

WHAT GOOD LOOKS LIKE

Every circuit has a reference number, a business-grade SLA, and 24/7 monitoring with twelve months of uptime history. You know the physical path into the building — and your ISP tells you about degradation before your users do.

SECTION 01 SCORE _____ / **10** *Aim for 8+. Below 6 = primary connection / monitoring gap.*

NOTES / OWNER / TARGET DATE

02

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)*.

THE SHARED-DUCT TRAP

Two ISPs that both ride the same physical fibre into the same street cabinet are not redundant. Confirm a diverse entry route and, ideally, a different technology — 4G/5G against fibre — so a single physical fault cannot take both connections down.

SECTION 02 SCORE _____ / 10 *Aim for 8+. Below 6 = no genuine independence.*

NOTES / OWNER / TARGET DATE

03

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.

WHAT GOOD LOOKS LIKE

A dual-WAN firewall fails over automatically in under thirty seconds on health-check failure across multiple external targets, alerts the team, logs the event, and fails back only once the primary is proven stable.

SECTION 03 SCORE _____ / **10** *Aim for 8+. Below 6 = failover not automatic.*

NOTES / OWNER / TARGET DATE

04

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.

DON'T LET DNS UNDO YOUR FAILOVER

Long TTLs and hard-coded public IPs are the quiet killers of a working failover — inbound traffic keeps pointing at the dead circuit. Check TTLs, dynamic DNS, VPN re-establishment and MX/SPF before you need them.

SECTION 04 SCORE _____ / **10** *Aim for 8+. Below 6 = DNS / routing gap.*

NOTES / OWNER / TARGET DATE

05

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.
- ☐ Monthly **performance reports** are generated comparing actual uptime and performance against SLA targets.
- ☐ Test results and monitoring data are **reviewed in quarterly IT review meetings** with actions tracked to completion.

UNTESTED = UNRELIABLE

Failover that has never been tested under real conditions is a hope, not a control. Schedule quarterly pull-the-plug tests, record switch and failback times, and review the trend in your IT meetings.

SECTION 05 SCORE _____ / **10** *Aim for 8+. Below 6 = untested failover.*

NOTES / OWNER / TARGET DATE

06

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.

A CALM OUTAGE IS A PLANNED OUTAGE

When the line drops, the team should reach for a runbook, not improvise. Documented ISP fault numbers, an escalation matrix, a staff comms template and a post-incident review turn chaos into a process.

SECTION 06 SCORE _____ / **10** *Aim for 8+. Below 6 = no incident plan.*

NOTES / OWNER / TARGET DATE

Σ

Audit score summary & action plan

Transfer the score for each section into the table. Set a priority (H/M/L) based on the gap to target. Anything below 6 is a candidate for the top-3 actions below.

#	AUDIT AREA	SCORE / 10	PRIORITY
01	Primary Connection Health	_____ / 10	☐ H ☐ M ☐ L
02	Secondary Connection Setup	_____ / 10	☐ H ☐ M ☐ L
03	Automatic Failover Configuration	_____ / 10	☐ H ☐ M ☐ L
04	DNS & Routing Resilience	_____ / 10	☐ H ☐ M ☐ L
05	Testing & Monitoring	_____ / 10	☐ H ☐ M ☐ L
06	Incident Response Procedures	_____ / 10	☐ H ☐ M ☐ L
Σ	**TOTAL SCORE**	_____ / 60	—

Score interpretation

48–60	**Excellent.** Your failover and redundancy strategy is robust. Focus on continuous testing and emerging risks.
36–47	**Good foundation, gaps exist.** Prioritise any area scoring below 6 with owners and deadlines.
Below 36	**Significant gaps** that put business continuity at risk. Consider an urgent review with a connectivity specialist.

Priority actions & sign-off

Translate your total score into a small number of next steps. The goal is one page of decisions, not a wish list — assign an owner and a date to each.

Top 3 priority actions

01 _____

02 _____

03 _____

Additional notes

_____

_____

_____

_____

AUDIT COMPLETED BY _____ DATE _____ NEXT REVIEW DUE _____

Need help building resilient connectivity?

Cloudswitched designs and manages dual-WAN failover, diverse circuits and 4G/5G backup for UK SMEs — with monitoring, quarterly testing and a documented incident response plan.

info@cloudswitched.com

cloudswitched.com/services/connectivity

CLOUDSWITCHED

IT SUPPORT & PROJECT SERVICES

info@cloudswitched.com

New London House, 6 London St
London EC3R 7LP · United Kingdom