

FREE RESOURCE — VERIFICATION CHECKLIST

Post-Move IT Verification Checklist

Six critical areas to verify after an office move — network, WiFi, servers, phones, workstations and security. Tick every check that is fully operational, score each area, and commit to top-three actions before declaring the move complete.

6

CRITICAL
AREAS
TO VERIFY

51

VERIFICATION
CHECKS

48h

TARGET
WINDOW
POST-MOVE

Fillable

TICK & TYPE
IN ANY VIEWER

NETWORK

SERVERS

COMMS

SECURITY

PREPARED FOR

Cloudswitched Knowledge
Library

PREPARED BY

Cloudswitched Ltd.

VERSION

2026 Edition

FORMAT

Interactive PDF

00

How to use this checklist

Start this checklist **immediately after the move is complete** and work through the six sections in order with your IT team or managed service provider on site. Tick every check that is **fully operational** — not partially, not "we'll fix that tomorrow", but in production and verifiable from a user's desk today. Then award each section a score out of 10 based on how many checks you can confidently tick.

All checks should be verified **within 48 hours** of the move. Anything that cannot be resolved on the day should be logged as an incident with a clear owner and deadline on the action items page at the back. 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 go/no-go gate for a UK SME office move covering the six IT areas that almost always uncover residual problems in the 48 hours after a relocation — network and connectivity, WiFi and wireless, servers and core services, phone system and communications, workstations and end-user devices, security and compliance. Use it to verify the move was successful, not to plan it (the move itself sits earlier in your relocation programme).

SCORING GUIDANCE

Award one point per check where you have evidence the system is fully operational — a successful test, a clean log, a user confirmation, a working call. Half measures do not score. Round each section to the nearest whole number out of 10 and carry it forward to the summary on the last page. Any section below 6 means the move is not yet complete in that area.

The six verification areas

- **01 Network & Connectivity** — circuits, firewall, VLANs, DNS/DHCP, VPN, monitoring.
- **02 WiFi & Wireless** — APs, coverage, signal strength, corporate vs guest, roaming.
- **03 Servers & Core Services** — AD, file shares, email, LOB apps, print, backup jobs.
- **04 Phone System & Communications** — desk phones, DDIs, voicemail, IVR, video, MTRs.
- **05 Workstations & End-User Devices** — PCs, monitors, docks, peripherals, printers, drives.
- **06 Security & Compliance** — firewall audit, physical security, UPS, EDR, SIEM, temp access.

01

Network & Connectivity

Verify every network connection, internet circuit and piece of core infrastructure is operational from the new site. Until this section is green, nothing else really matters — users with no DNS or DHCP cannot meaningfully test anything downstream.

- ☐ Primary **internet circuit** is live with expected bandwidth (*run a speed test and compare to contracted speed*).
- ☐ **Secondary / backup internet** connection is active and failover has been tested by pulling the primary.
- ☐ All **network switches** are powered on, patched, and showing expected port connectivity in the management console.
- ☐ **Firewall** is operational with all rules, NAT translations and VPN configurations intact — no temporary "allow any" rules left in place.
- ☐ All **VLANs** are configured correctly — test connectivity between VLANs and verify isolation where required.
- ☐ **DNS resolution** works for both internal and external domains from every network segment.
- ☐ **DHCP** is issuing correct IP addresses, gateways and DNS servers on all VLANs.
- ☐ All **network ports** at workstation locations are tested and patched to the correct switch ports.
- ☐ **VPN** is accessible for remote workers — test from an external connection, not from the new office.
- ☐ Network **monitoring tools** are receiving data from every device at the new site.

WHAT GOOD LOOKS LIKE

Both circuits live with documented bandwidth. Firewall, switches and APs all reporting into the monitoring stack from their new IP addresses. A failover test was actually performed, not just assumed. The phrase "we will fix the VPN tomorrow" appears nowhere in the move log.

SECTION 01 SCORE / 10

Aim for 9+. Below 6 = move is not complete here.

02

WiFi & Wireless

Verify wireless coverage, performance and security across the entire new office — including the corners, meeting rooms and breakout spaces nobody thought to test. A WiFi analyser app on a phone is enough; walk every working area before signing this off.

- ☐ All **access points** are powered on, broadcasting the correct SSIDs and managed by the controller.
- ☐ **WiFi coverage** is adequate in all work areas, meeting rooms, breakout spaces and reception — no dead zones.
- ☐ **Signal strength** is ≥ -65 dBm in all primary work areas (*use a WiFi analyser to verify each desk cluster*).
- ☐ **Corporate WiFi** authenticates users correctly via 802.1X or WPA3-Enterprise.
- ☐ **Guest WiFi** is isolated from the corporate network and provides internet-only access.
- ☐ **Bandwidth per AP** is sufficient under realistic load — test with multiple simultaneous users on the same AP.
- ☐ **Roaming** between access points works seamlessly without call drops or session drops.
- ☐ WiFi **channel allocation** is optimised to avoid interference (*check the controller for neighbouring networks*).

WATCH OUT FOR

"It works at my desk" is not coverage. Plaster, glass partitions, kitchens and stairwells routinely create -75 dBm dead zones that only appear when someone tries a Teams call from a sofa or a phone booth. Walk every floor with an analyser, not just the desks.

SECTION 02 SCORE / 10

Aim for 8+. Below 6 = coverage / roaming gap.

03

Servers & Core Services

Verify all server infrastructure and the core services your users rely on are operational from the new site. Files, email, line-of-business apps, print and scheduled jobs all need to be working **and** reporting in cleanly to monitoring before this section scores well.

- ☐ All **physical and virtual servers** are powered on, accessible and showing healthy status in management tools.
- ☐ **Active Directory** domain controllers are replicating correctly between all DCs (*check repadmin or equivalent*).
- ☐ **File shares** are accessible with correct permissions from every workstation — not just from IT's laptops.
- ☐ **Email** is flowing inbound and outbound — send test messages to and from external addresses, including one with an attachment.
- ☐ **Line-of-business applications** are accessible and have been tested by key users from their actual desks.
- ☐ **Database servers** are accessible and applications can read and write data correctly under realistic load.
- ☐ **Print servers** are operational and all networked printers are accessible to the correct user groups.
- ☐ **Backup jobs** have been reconfigured for the new site and the first post-move backup completed successfully (*verify, do not assume*).
- ☐ All **scheduled tasks** and automated processes are running on time and not stuck on the old site's IP addresses.

COMMON GAP: BACKUP PATHS

Backup jobs that worked perfectly at the old site routinely fail post-move because the target NAS, cloud endpoint or VPN tunnel still references the previous LAN. Run the first backup the night of the move and watch it complete — do not wait until Monday to discover three days of data are not protected.

SECTION 03 SCORE _____ / 10

Aim for 9+. Below 6 = service outage risk.

04

Phone System & Communications

Verify every telephone and communication channel is fully operational. With PSTN gone and almost every UK SME running cloud voice or VoIP, the most common post-move surprise is inbound calls routing to the wrong handset, dropped DDIs, or a dead meeting-room camera that nobody tested before the first client call.

- ☐ All **desk phones** are registered with the platform and showing the correct extension number on the display.
- ☐ **Inbound calls** to the main number(s) and all DDIs are routing to the correct user or hunt group.
- ☐ **Outbound calls** work from every handset — test local, national, mobile and one international number.
- ☐ **Voicemail** is operational and messages are being delivered (to the inbox or the handset) within the expected SLA.
- ☐ **Call recording** (if applicable) is functioning and recordings are being stored to the correct location with retention applied.
- ☐ **Auto-attendant / IVR** menus are working and routing to the correct departments — including out-of-hours and holiday routes.
- ☐ **Video conferencing** in every meeting room has been tested — cameras, microphones, speakers and screens all working.
- ☐ **Teams / Zoom** integration with meeting room systems has been tested with an external participant joining live.

TEST BEFORE THE FIRST CLIENT CALL

The first board call or client demo from the new office is not the time to discover the MTR camera is unbound, the room mic is muted at the firmware level, or the IVR still says "press 9 for our old reception". Schedule a deliberate test call from every meeting room to an external mobile before the office opens.

SECTION 04 SCORE _____ / 10

Aim for 8+. Below 6 = visible client impact.

05

Workstations & End-User Devices

Verify every user has a working setup at their new desk before they sit down for their first session. The biggest single source of post-move complaints is small things at the desk — a dead monitor port, a missing dock cable, a printer queue still pointing at the old print server.

- ☐ All **laptops and desktops** are powered on, on the corporate network and connecting to the domain or Entra ID.
- ☐ All **monitors** are connected and displaying at the correct resolution and refresh rate.
- ☐ **Docking stations** are functioning — USB ports, dual-display output, ethernet passthrough and power delivery to the laptop.
- ☐ All **peripherals** (keyboard, mouse, headset, webcam) are working and paired to the correct device.
- ☐ **Printers** are installed and users can print a test page to their nearest physical device.
- ☐ Users can access **all required applications** including Microsoft 365 / Google Workspace and line-of-business cloud services.
- ☐ **Mapped drives**, OneDrive sync and desktop shortcuts are working correctly — not stuck on the old paths.
- ☐ Users have received the **new office IT guide** — WiFi name, printer setup, helpdesk contact, post-move issue process.

DAY-ONE WALK-ROUND

Send a small team round every desk on day one with a checklist on a tablet. Five minutes per desk catches the missing HDMI cable, the dock without power, the wrong mouse — all of which generate three helpdesk tickets each if you wait for users to find them. This is the cheapest possible post-move quality control.

SECTION 05 SCORE _____ / 10

Aim for 8+. Below 6 = user productivity loss.

06

Security & Compliance

Verify every security measure that protected the old site is active at the new site — nothing degraded or temporarily relaxed for the move. Moves are a classic window for permissive firewall rules and admin accounts to be granted "just for today" and then quietly forgotten.

- ☐ **Firewall rules** have been audited post-move — no temporary permissive rules, any-any rules or move-only NAT entries left in place.
- ☐ **Physical security** of the server / comms room is active — door access control, CCTV coverage and the room is locked.
- ☐ **UPS** is protecting all critical infrastructure and has been tested with a controlled mains interruption.
- ☐ **Environmental monitoring** (temperature, humidity, water) is active and alerting in the server room.
- ☐ **Endpoint protection** (EDR / next-gen AV) is reporting in for all devices from the new site — no silent agents.
- ☐ **Security monitoring / SIEM** is receiving logs from all devices at the new location, with no source IPs orphaned.
- ☐ All **temporary admin access** granted for the move has been revoked and the audit log archived.
- ☐ A **vulnerability scan** has been run from the new site to verify no new exposures (open ports, weak ciphers, exposed admin).

REVOKE TEMP ACCESS ON THE DAY

Every move generates a handful of contractor accounts, shared admin credentials and "any-any" firewall rules so that engineers can get things working under pressure. If they are not revoked the day the move completes, they will still be active twelve months later when an auditor or attacker finds them. Close the loop the same day.

SECTION 06 SCORE / 10

Aim for 9+. Below 6 = exposed attack surface.



Verification score summary

Transfer the score for each section into the table. Set a priority (H/M/L) for any area that is not yet fully operational. Anything below 6 in any row means the move is not yet complete in that area — capture it on the next page as a top-three action.

#	VERIFICATION AREA	SCORE / 10	PRIORITY
01	Network & Connectivity	_____ / 10	☐ H ☐ M ☐ L
02	WiFi & Wireless	_____ / 10	☐ H ☐ M ☐ L
03	Servers & Core Services	_____ / 10	☐ H ☐ M ☐ L
04	Phone System & Communications	_____ / 10	☐ H ☐ M ☐ L
05	Workstations & End-User Devices	_____ / 10	☐ H ☐ M ☐ L
06	Security & Compliance	_____ / 10	☐ H ☐ M ☐ L
Σ	TOTAL SCORE	_____ / 60	—

Score interpretation

50–60

Move complete. Sign off, archive the move log and close out temporary access. Schedule a 30-day post-move review with users to catch anything that only shows up under sustained load.

36–49

Operational, with gaps. Capture the open items on the next page with owners and deadlines — do not sign off until every section is at 6+ and any high-priority gap has a date.

Below 36

Move not yet complete. Escalate now — users are running on a partially-built site and risk is concentrated. Roll forward to a full remediation pass before declaring the move closed.

A NOTE ON THE 48-HOUR WINDOW

Most post-move IT problems — firmware regressions, DNS edge cases, intermittent WiFi roaming — only surface under real users on real days. Aim to be fully green within 48 hours so anything you see in week one is a genuine bug, not a setup error.



Priority actions & sign-off

Translate the gaps into a small number of next steps and assign them. The goal is one page of decisions, not a wish list. Sign off only when every section is at 6 or better, every temporary access has been revoked and the first post-move backup has completed cleanly.

Top 3 priority actions

01

02

03

Additional notes

COMPLETED BY

DATE

NEXT REVIEW DUE

Need post-move IT support?

Cloudswitched runs full post-move verification visits for UK SMEs — network, WiFi, servers, phones, workstations and security — with fixed-price remediation for anything that fails the gate.

info@cloudswitched.com

cloudswitched.com/services/it-support



CLOUDSWITCHED

IT SUPPORT & OFFICE MOVES

info@cloudswitched.com

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