RUPE NETWORKS

DOC-NCL-2026-01
EDITION 1 · APRIL 2026

FREE INFRASTRUCTURE RESOURCE — RUPE NETWORKS

NETWORK READINESS CHECKLIST

A critical self-assessment framework for IT managers, network teams, and businesses planning infrastructure changes, technology adoption, or compliance preparation.

> "Most network problems don't appear overnight. They accumulate — quietly, one undocumented change, one missed firmware update, and one unchecked alert at a time."

rupe-networks.co.uk
contact@rupe-networks.co.uk

GAPS IDENTIFIED?
REQUEST A FREE ASSESSMENT →

// INTRODUCTION

HOW TO USE THIS CHECKLIST

This checklist is designed for IT managers, operations teams, and business leaders who want to understand the true state of their network before embarking on a change programme, preparing for compliance, or responding to recurring operational problems.

Each item reflects the critical thinking RUPE Networks applies to every engagement. These are not theoretical best practices – they are the checks that prevent real outages, failed technology deployments, and costly remediation projects. A gap in this list is a gap in your operational resilience.

WHO IS THIS FOR?

IT managers, network leads, and technical decision-makers evaluating infrastructure health or planning a technology programme.

WHEN TO USE IT

Pre-project (SD-WAN, cloud migration, office move), new IT appointment, Cyber Essentials preparation, or scheduled infrastructure review.

HOW TO USE IT

Work through each section. Mark items as complete, partial, or outstanding. Use priority badges to sequence your remediation effort.

CRITICAL Active risk – address immediately

HIGH Important – plan within 90 days

STANDARD Best practice – address within 6 months

COMMON FINDING: Most businesses discover their largest risks aren't in the security section – they're in monitoring, documentation, and operational readiness. These are the gaps that turn manageable faults into major outages.

The eight sections mirror the areas RUPE Networks evaluates in a formal infrastructure assessment. A "yes" on everything is rarely the starting point – the value is understanding where the gaps are, why they exist, and which carry the most operational risk.

RUPE NETWORKS: If you identify gaps you can't address internally – whether that's an infrastructure audit, remediation planning, or a full deployment project – we provide hands-on network engineering consultancy with no retainer requirement. Engage for one project or many.

// SECTION 01

DOCUMENTATION & INVENTORY

The first question in any network assessment isn't technical — it's whether the documentation reflects reality. In most environments, the honest answer is somewhere between "partially" and "not really." This section establishes your documentation baseline.

- [ ] **Current topology diagram exists and reflects actual L2/L3 state** — CRITICAL
  Shows VLANs, uplinks, inter-device connections, and subnet boundaries — not the diagram from the original install five years ago. A diagram that doesn't show routing structure isn't a network diagram, it's decoration.

- [ ] **IP address management (IPAM) documented and current** — HIGH
  Spreadsheet or dedicated tool — either is acceptable, but it must exist and be maintained. Discovering devices by running a subnet scan is not IPAM.

- [ ] **VLAN register complete — name, purpose, and subnet per VLAN** — HIGH
  If you can't identify VLAN 40 without logging into a switch, the register is inadequate. VLANs without documented purposes accumulate and create security blind spots.

- [ ] **Configuration backups exist for all managed network devices** — CRITICAL
  If a core switch failed today, could you restore the configuration from backup in under an hour? Test this — don't assume. Backups that exist but haven't been tested are half a backup.

- [ ] **Physical cabling records and patch schedule maintained** — STANDARD
  What connects to what, from which port, to which port. In a comms room that's been in service for several years, the common answer is "sort of." That's a troubleshooting liability.

- [ ] **As-built documentation updated after every infrastructure change** — HIGH
  Documentation debt accumulates faster than technical debt. Every undocumented change is a time bomb for the next engineer who needs to work on the network under pressure.

- [ ] **ISP circuit IDs, SLAs, and support contacts documented** — HIGH
  Circuit reference numbers, escalation paths, and contract end dates must be accessible immediately during an outage — not buried in an email thread from the original procurement.

- [ ] **DNS and DHCP architecture documented** — STANDARD
  Which servers or devices are authoritative DNS? Where is DHCP served from, and what are the scopes? Undocumented DNS changes are a common source of silent failures.

RUPE NETWORKS: We routinely inherit environments where topology diagrams are multiple infrastructure generations out of date. Our assessments produce current, accurate as-built documentation as a deliverable — not a byproduct. rupe-networks.co.uk

// SECTION 02

HARDWARE & FIRMWARE AUDIT

> Firmware gaps are not cosmetic. Vendors release security patches alongside feature updates — a switch running firmware from 2021 is missing several years of CVE fixes. EOL hardware in production is an unmanaged risk, not a budget decision.

- [ ] **Full hardware inventory exists — make, model, serial, location, role** — CRITICAL
  Includes switches, routers, firewalls, wireless APs, and any network-connected appliances. Without this, you cannot manage firmware or plan replacement cycles.

- [ ] **Firmware versions recorded and compared against vendor current release** — CRITICAL
  For each device: what is running, and what is current? Devices two or more major versions behind are a priority for remediation — not "when convenient."

- [ ] **EOL and EOS dates recorded for all devices** — HIGH
  End-of-life (no longer manufactured) and end-of-support (no further security patches) dates must be tracked. EOL hardware in production represents unpatched vulnerability exposure.

- [ ] **EOL and EOS hardware is in a documented replacement plan** — HIGH
  Budget cycles are real. The point of flagging is to get obsolete hardware into a remediation plan with a named owner and a target date — not to demand immediate replacement.

- [ ] **No consumer-grade equipment deployed in production roles** — CRITICAL
  A home router pressed into production service because something was needed quickly is a persistent finding. Consumer hardware lacks enterprise management, VLAN support, and reliable firmware patching.

- [ ] **Warranty status known for all critical devices** — STANDARD
  Expired hardware warranties mean next-business-day replacement support is gone. Out-of-warranty failures in core switching or firewall equipment can cause extended outages.

- [ ] **Planned firmware update schedule defined and tested** — HIGH
  Firmware updates should be planned, tested in a maintenance window, and documented. Ad-hoc updates applied without testing or rollback planning are a common change-related incident root cause.

⚠ **COMMON FINDING:** In most SMB assessments, at least one device is end-of-support — most commonly wireless access points or access layer switches that have been quietly running since the original site fit-out. These are often unknown risks because nobody checked.

// SECTION 03

SECURITY POSTURE

Security findings in network audits are rarely sophisticated. They're defaults that were never changed — community strings left as "public," management interfaces reachable from user VLANs, firewall rules that haven't been reviewed since the original deployment.

- [ ] **Default credentials eliminated on all managed devices** — CRITICAL
  Switches, access points, management interfaces, OOB tools. This is a basic finding in a significant proportion of SMB audits. Every default credential is an open door.

- [ ] **SNMP community strings changed or SNMPv1/v2c disabled** — CRITICAL
  SNMP v2c with "public" is effectively unauthenticated read access to device configuration data. Migrate to SNMPv3 with authentication and encryption, or disable SNMP where not required.

- [ ] **Unused switch ports administratively disabled** — HIGH
  An enabled, unassigned port in a reception area or meeting room is a physical access risk. Anyone who can plug in a cable can reach the network. Disable all unused ports.

- [ ] **Device management interfaces access-controlled to management VLAN** — CRITICAL
  Switch and firewall management IPs should be reachable only from a dedicated management VLAN or jump host. If management interfaces are on the general user LAN, that's a network design gap.

- [ ] **Firewall policies reviewed within the last 12 months** — HIGH
  Rules accumulate. Old policies for systems that no longer exist, temporary rules made permanent, broad "allow" rules for troubleshooting never removed. Annual review minimum.

- [ ] **VPN encryption — no deprecated ciphers in use** — HIGH
  3DES, RC4, MD5, DH groups 1 or 2 are deprecated. Check IKEv1/v2 proposals directly on the device — dashboard summaries do not reliably surface weak cipher configurations.

- [ ] **Guest wireless isolated from corporate infrastructure** — CRITICAL
  Guest SSID must be on a separate VLAN with firewall rules blocking access to corporate resources. Guest traffic should exit directly to internet without traversing internal switching.

- [ ] **Remote access assessed — MFA enforced on all remote entry points** — CRITICAL
  VPN, RDP, and any remote management portal must have multi-factor authentication. Credentials-only remote access is a known attack vector regardless of password complexity.

- [ ] **Cyber Essentials controls assessed against current network state** — STANDARD
  Boundary firewalls, patching, access control, malware protection, and secure configuration. Cyber Essentials is the baseline — not the ceiling.

// SECTION 04

SD-WAN READINESS ASSESSMENT

SD-WAN is a significant capability shift — not just a product swap. The companies that get the most from SD-WAN deployments are those that understand their application requirements, underlay quality, and skill gaps before they commit to a platform.

- [ ] **Current WAN topology documented — circuits, carriers, speeds, and costs** — CRITICAL

  You cannot design an SD-WAN overlay without understanding your current underlay. Include contract end dates — WAN circuit procurement timelines are often longer than expected.

- [ ] **Application requirements profiled — latency, jitter, and bandwidth per app** — CRITICAL

  SD-WAN delivers value through application-aware routing. Without a clear application profile, you cannot define meaningful SLA thresholds or steering policies. VoIP and UC have different requirements to bulk file transfer.

- [ ] **Underlay circuit quality measured — packet loss, jitter, and latency baselined** — HIGH

  SD-WAN cannot compensate for chronically poor underlay quality. If your current circuits have sustained packet loss above 0.5%, that needs resolving before or alongside an SD-WAN deployment.

- [ ] **Failover requirements defined — RTO and RPO for each site** — HIGH

  How quickly does a site need to fail over to a backup circuit? What traffic can be degraded versus what must remain available? These requirements drive SLA threshold configuration.

- [ ] **Existing edge hardware assessed — SD-WAN capable or replacement required?** — HIGH

  Not all existing routers or firewalls can support SD-WAN overlay functions. Assess whether a software upgrade suffices or whether new edge hardware is required — this drives a significant portion of project cost.

- [ ] **Management platform and licensing costs factored into budget** — HIGH

  SD-WAN overlay management (FortiManager, Cisco vManage, etc.) carries ongoing licensing costs. These are frequently underestimated or omitted from initial project budgets.

- [ ] **Internal team skills assessed — SD-WAN administration capabilities evaluated** — HIGH

  SD-WAN platforms differ significantly from traditional routing. The operational model changes. Training or external support requirements should be scoped before go-live, not after the first incident.

- [ ] **Failover and SLA health checks tested before handover** — CRITICAL

  Physical failover testing is non-negotiable. Failover that looks correct in the dashboard and fails under real traffic is a common deployment gap — test it before the maintenance window closes.

RUPE NETWORKS: We design and deploy SD-WAN solutions using Fortinet and Alcatel-Lucent Enterprise platforms. We scope the underlay, design the overlay, and test failover — before and after handover. No vendor lock-in.

// SECTION 05

PHYSICAL LAYER & CABLING

Physical layer problems are the most underestimated source of intermittent network faults. Marginal cable runs, uncertified cabling, and overloaded comms rooms cause faults that are difficult to diagnose, expensive to fix, and entirely preventable.

- [ ] **Structured cabling installed to minimum Cat5e / Cat6 standard** — HIGH

  Cat5e supports 1Gbps at up to 100m. Cat6 supports 10Gbps at shorter distances and provides better headroom for high-density wireless and future uplink requirements.

- [ ] **Cabling tested and certified with test results retained** — HIGH

  Installed cabling should have Fluke or equivalent certification test results on file. Without test evidence, you have no baseline to investigate future performance issues.

- [ ] **All cables labelled consistently at both ends** — STANDARD

  Unlabelled or inconsistently labelled cabling in a comms room significantly increases fault resolution time. During a major incident, spending 20 minutes tracing cables is not acceptable.

- [ ] **Cable management in place — no unmanaged bundles or cable droops** — STANDARD

  Poor cable management increases the risk of accidental disconnections, reduces airflow in cabinets, and makes fault diagnosis significantly more difficult.

- [ ] **UPS in place for all network equipment in comms rooms** — CRITICAL

  A brief power interruption without UPS causes a cold restart of all network equipment simultaneously – the worst possible failure mode for a network that supports telephony or time-sensitive applications.

- [ ] **UPS battery health tested and replacement schedule in place** — HIGH

  A UPS with a failed battery provides no protection. Battery health should be tested annually. Most UPS batteries have a 3–5 year service life regardless of usage.

- [ ] **Comms room temperature and humidity within acceptable range** — HIGH

  Network equipment should operate below 35°C ambient. Overheating is a leading cause of premature hardware failure and intermittent interface errors that don't immediately trace back to environmental causes.

- [ ] **Fibre runs documented — type, length, connector standard** — STANDARD

  For inter-building or inter-floor fibre: single-mode vs multimode, connector type (LC, SC), and run length documented. Critical when specifying SFP modules for upgrades or replacements.

// SECTION 06 – OFTEN THE BIGGEST GAP

NETWORK MONITORING & NMS

> An unmonitored network is a network you're operating blind. This section goes beyond "is an NMS in place" – it examines whether monitoring is comprehensive, alerts are actionable, and the team actually responds when something surfaces.

- [ ] **NMS platform deployed – all devices discovered and polled** — CRITICAL
  PRTG, LibreNMS, Zabbix, Auvik, SolarWinds, or equivalent. Every managed network device must be visible to the monitoring platform – not just routers and firewalls.

- [ ] **Interface up/down alerting configured for all critical links** — CRITICAL
  WAN uplinks, inter-site links, core uplinks, and server-facing interfaces must generate an alert on state change. Discovering a link is down via a user complaint is not monitoring – it's luck.

- [ ] **Bandwidth utilisation trending captured per interface** — HIGH
  Inbound and outbound utilisation trending enables capacity planning and early identification of saturation. Without historical trending, you cannot distinguish a performance issue from a capacity problem.

- [ ] **Interface error counters monitored – CRC errors, discards, input errors** — HIGH
  Incrementing error counters on an interface indicate a physical layer problem – often before users notice any impact. This data is invisible without SNMP polling of interface statistics.

- [ ] **CPU and memory thresholds configured on routers, switches, and firewalls** — HIGH
  High CPU on a firewall or core switch degrades performance before causing an outage. Threshold-based alerts enable pre-emptive investigation rather than reactive incident response.

- [ ] **Syslog collection configured – all devices forwarding to a central repository** — CRITICAL
  Syslog is your network's event record. Without centralised collection, you cannot correlate events across devices, and log evidence is lost when a device reboots or fills its local buffer.

- [ ] **SNMP trap receivers configured – devices sending traps to NMS** — STANDARD
  SNMP traps provide near-real-time event notification for conditions like interface state changes, hardware failures, and authentication failures – faster than polling-based discovery.

- [ ] **Alert escalation path defined – who gets notified, in what order, by what method** — CRITICAL
  An alert that fires to a shared mailbox that nobody monitors is not an alert – it's a log entry. Define named recipients, escalation tiers, and notification methods (email, SMS, Teams, PagerDuty).

- [ ] **Out-of-hours alerting coverage defined and tested** — CRITICAL
  Most outages occur outside business hours. If no one is configured to receive or respond to alerts overnight or at weekends, your effective monitoring coverage is 9–5, Monday to Friday.

// SECTION 06 – CONTINUED

MONITORING & NMS – ADVANCED CHECKS

Beyond basic up/down monitoring, a mature NMS implementation provides traffic visibility, proactive capacity data, and a process for acting on what it surfaces – not just an inbox full of unreviewed alerts.

- [ ] **Alert fatigue assessed – all active alerts are actionable** HIGH

  An NMS that generates hundreds of low-signal alerts trains teams to ignore them. Review active alerts: if the response to most is "acknowledged and ignored," the alerting configuration needs tuning, not more alerts.

- [ ] **Maintenance windows handled in NMS – alert suppression during planned work** STANDARD

  Planned maintenance that triggers mass alerts desensitises the team to real alerts. Schedule suppression windows for planned downtime so alerts remain meaningful.

- [ ] **NetFlow or sFlow configured for traffic visibility and anomaly detection** STANDARD

  Flow data identifies top talkers, unusual traffic patterns, and potential security anomalies. SNMP bandwidth counters tell you how much – NetFlow tells you who and what.

- [ ] **WAN circuit SLA reporting available – loss, latency, and jitter tracked** HIGH

  ISP SLA reporting is not the same as independent measurement. Operate your own latency and packet loss monitoring against the ISP circuit – this is your evidence base for SLA claims and circuit fault escalations.

- [ ] **NMS itself is monitored – "who watches the watcher?"** HIGH

  If your NMS platform goes offline or stops polling, you will not receive alerts about infrastructure failures. An external health check for the NMS itself is a basic requirement that is frequently missed.

- [ ] **NMS credentials reviewed – access is least-privilege and documented** HIGH

  SNMP community strings and SNMP v3 credentials used by the NMS should be documented, access-controlled, and rotated when personnel change. NMS access provides read access to device configurations.

- [ ] **Wireless client density and RSSI monitoring in place** STANDARD

  For environments with significant wireless use: RSSI, channel utilisation, and client count trending per AP enables proactive capacity planning and identifies coverage degradation before users report it.

⚠ COMMON FINDING: "We have PRTG but nobody checks it" is the most common monitoring answer in SMB assessments. An NMS that's installed but unreviewed is not monitoring – it's a dashboard no-one looks at. The process matters as much as the tool.

RUPE NETWORKS: We design and implement NMS platforms tailored to your environment – from initial device discovery through alert tuning, escalation path configuration, and team handover. A monitoring platform built by us is built to be used, not inherited.

// SECTIONS 07 & 08

PERFORMANCE, CAPACITY & OPERATIONS

Performance issues in SMB networks are rarely about headline bandwidth – they're about mismatches between what's deployed and what's needed. Operational readiness determines whether infrastructure problems stay manageable or become incidents.

// PERFORMANCE & CAPACITY

- [ ] **Uplink utilisation baselined during peak hours** — HIGH
  Core-to-distribution and distribution-to-access uplinks. If uplinks are regularly hitting 70–80% utilisation during business hours, that's a capacity planning item – not a fault, but an impending one.

- [ ] **Internet circuit headroom assessed – current average vs. contracted capacity** — HIGH
  Most ISPs provide utilisation data via portal or SNMP. If average utilisation exceeds 60% of contracted capacity during business hours, circuit upgrade should be in the procurement pipeline.

- [ ] **Speed mismatches identified – gigabit-capable devices on 100Mbps ports** — STANDARD
  A common finding on older access switches. A server or primary workstation connected at 100Mbps where the hardware supports 1Gbps is a silent performance ceiling that's trivially fixable.

- [ ] **QoS configured end-to-end for voice and video traffic** — HIGH
  An unconfigured switch will not prioritise voice traffic over a concurrent bulk file transfer. Check DSCP markings, trust boundaries, and queue configurations on every switch in the voice path.

- [ ] **Wi-Fi coverage validated – RSSI above -72dBm across all working areas** — STANDARD
  Coverage maps from the original deployment don't reflect changed office layouts, new meeting rooms, or increased device density. Walk the site with a survey tool and verify current coverage.

// OPERATIONAL READINESS

- [ ] **Change management process defined – all changes logged with rollback plan** — CRITICAL
  The majority of network outages are change-related. A change log with pre-change backups and a defined rollback procedure is the single most effective operational risk control available.

- [ ] **Runbooks exist for common operational tasks and failure scenarios** — HIGH
  ISP circuit escalation, firewall failover, AP replacement, core switch recovery. Runbooks reduce mean time to resolution and reduce dependency on one person's knowledge.

- [ ] **DR/BCP network recovery procedure documented and tested** — HIGH
  A network recovery plan that hasn't been tested is a hypothesis. Annual testing of the recovery procedure under realistic conditions is the only way to validate that it works.

- [ ] **Skills and knowledge dependencies assessed – single points of human failure identified** — HIGH
  If one person leaves and network knowledge walks out with them, that's an operational risk. Document knowledge, not just configurations. Consider skills gap coverage for planned absences.

// WHAT HAPPENS NEXT

YOU'VE IDENTIFIED GAPS. NOW WHAT?

Most organisations that complete this checklist identify between three and eight significant gaps. Some are straightforward to close internally. Others – particularly around monitoring architecture, SD-WAN design, or security hardening – benefit from specialist input to get right first time.

RUPE Networks provides network engineering consultancy to UK businesses. We work on specific engagements – no retainer, no lock-in. Whether that's a one-day infrastructure assessment, a full SD-WAN deployment, or NMS architecture and implementation, we engage at the level you need.

NETWORK ASSESSMENT

Infrastructure audit covering documentation, hardware, security, and operational readiness. Findings report with prioritised remediation recommendations.

SD-WAN DESIGN & DEPLOY

End-to-end SD-WAN projects using Fortinet and Alcatel-Lucent Enterprise. Underlay assessment, overlay design, deployment, and handover.

NMS ARCHITECTURE

Monitoring platform design, deployment, and tuning. Interface monitoring, alerting, syslog, and flow analysis configured for your environment.

SECURITY HARDENING

Firewall policy review, segmentation assessment, Cyber Essentials preparation, and access control remediation. FortiGate-certified engineers.

SMART HANDS

On-site rack and stack, cabling, and equipment commissioning across the UK. Structured cabling installation and certification.

SUBCONTRACT RESOURCE

White-label network engineering for MSPs, IT teams, and partners. Skilled engineers available for projects requiring specialist network expertise.

WEBSITE
rupe-networks.co.uk

EMAIL
contact@rupe-networks.co.uk

PHONE
020 3011 4490

RUPE Networks Limited is a UK-based network engineering consultancy providing specialist infrastructure services to businesses across the UK. Certified in Fortinet, Alcatel-Lucent Enterprise, and Cisco technologies. All engagements are project-based – no retainer or minimum commitment required.