Organisation: [Name] | Site: [Location] | Audited by: [Name]

Date: [Date] | Next audit due: [Date]

Network Infrastructure

[ ] Network diagram exists and is current (dated within 12 months)
[ ] All switches, routers, and access points documented (make, model, firmware)
[ ] Firewall rules reviewed, documented, and approved
[ ] Unused switch ports disabled
[ ] Guest Wi-Fi isolated from corporate network on separate VLAN
[ ] Remote access solution documented (VPN / RDP gateway / ZTNA)
[ ] Internet connection documented (provider, speed, redundancy/failover)
[ ] DNS settings confirmed, DNS filtering in place
[ ] Network monitoring tool in place and alerting confirmed

Endpoints

[ ] Full endpoint inventory completed and current
[ ] All endpoints running supported OS (no end-of-life Windows or macOS)
[ ] All endpoints enrolled in patch management
[ ] Patch compliance rate: ____%
[ ] Endpoint protection (AV/EDR) deployed and reporting centrally
[ ] Full disk encryption enabled on all laptops and portable devices
[ ] Local admin rights reviewed and minimised
[ ] Inactive user accounts disabled or removed
[ ] Mobile device management (MDM) in place for mobile devices

Servers and Cloud

[ ] Server inventory completed (on-prem and cloud/hosted)
[ ] All server OS versions documented, EOL flagged
[ ] Server roles and dependencies documented
[ ] Virtualisation platform documented and licenced correctly
[ ] Cloud services inventory completed
[ ] Cloud admin accounts reviewed (MFA enforced, no shared accounts, least privilege applied)
[ ] Microsoft 365 / Google Workspace admin roles reviewed
[ ] Cloud spend reviewed against usage

Backup and Recovery

[ ] Backup solution documented (what, where, how often)
[ ] All critical systems and data within backup scope
[ ] Last successful backup confirmed for each system
[ ] Last restore test date: ____ (recommended: quarterly minimum)

[ ] Offsite or immutable cloud copy confirmed
[ ] RTO and RPO defined and agreed with client
[ ] Backup monitoring alerts configured

Security

[ ] MFA enabled on all email accounts
[ ] MFA enabled on all cloud admin accounts
[ ] MFA enabled on VPN and remote access
[ ] Password manager in use across the organisation
[ ] Email filtering in place (anti-spam, anti-phishing, attachment sandboxing)
[ ] DNS filtering in place
[ ] EDR solution deployed and reporting to central console
[ ] SIEM or log aggregation in place (or documented decision not to)
[ ] Security awareness training in place (last session date: ____)
[ ] Vulnerability scanning completed (last scan date: ____)
[ ] Incident response plan documented and tested
[ ] Cyber insurance confirmed (provider, policy number, renewal date: ____)

Capacity and Growth

[ ] Current storage utilisation documented (servers, cloud, backup)
[ ] Projected growth discussed with client (12-month horizon)
[ ] Network bandwidth adequate for current and planned workloads
[ ] Any AI tools or new workloads assessed for infrastructure impact
[ ] Hardware refresh schedule reviewed (flag anything over 5 years old)

Compliance and Documentation

[ ] IT policies documented (acceptable use, BYOD, data retention, remote working)
[ ] Data classification understood and documented
[ ] Regulatory requirements identified (HIPAA, PCI-DSS, SOC 2, ISO 27001, other)
[ ] Vendor and third-party contact list current
[ ] Software licence register current and compliant
[ ] IT documentation stored centrally and accessible to MSP team

Summary Findings

Area	Rating (Red/Amber/Green)	Key Issues
Network		
Endpoints		
Servers and cloud		
Backup and recovery		

Area	Rating (Red/Amber/Green)	Key Issues
Security		
Capacity and growth		
Compliance		

Prioritised Remediation Plan

Action	Risk level (Critical/High/Med/Low)	Owner	Target date	Est. cost

Audit Sign-Off

Audited by: _____ Date: _____

Reviewed by (client): _____ Date: _____