VoIP System Readiness Audit Checklist

Comprehensive audit of your VoIP infrastructure covering network readiness, QoS, hardware, platform configuration, call quality, security, and disaster recovery — 65+ items.

7	65+	Score	Free
AUDIT AREAS	ITEMS TO CHECK	EACH SECTION OUT OF 10	PRINT & USE NO STRINGS

How to Use This Checklist

Complete this audit with your IT team or VoIP provider. Test call quality using real calls to external numbers, not just internal extensions. Score each section out of 10 and create an action plan for areas scoring below 6.

1 Network Infrastructure Assessment

VoIP performance is entirely dependent on your network. A poor network guarantees poor call quality regardless of the VoIP platform.

- [ ] Internet connection has **sufficient bandwidth** for concurrent voice calls plus data traffic (allow 100 Kbps per concurrent call minimum)
- [ ] A **dedicated VLAN for voice traffic** separates VoIP from data traffic to prevent congestion impacting call quality
- [ ] Network switches support **802.1p/Q VLAN tagging** and are configured to prioritise voice traffic on the dedicated voice VLAN
- [ ] The **firewall is configured to prioritise SIP and RTP traffic** with appropriate QoS markings applied at the network edge
- [ ] All network equipment between the phones and internet connection supports **Power over Ethernet (PoE)** for IP handsets
- [ ] Network **latency is measured at below 150ms** end-to-end to the VoIP provider's data centre (target: below 80ms for best quality)
- [ ] **Jitter is consistently below 30ms** and ideally below 15ms during peak business hours
- [ ] **Packet loss is at or near 0%** — even 1% packet loss causes audible quality degradation on voice calls
- [ ] SIP ALG (Application Layer Gateway) is **disabled on the router and firewall** as it commonly causes VoIP registration and audio issues
- [ ] The network has been tested with a **VoIP readiness assessment tool** (e.g., Ooma, VoIP Spear, or provider-specific tools)

Section Score: ____/10

2 Bandwidth & QoS Configuration

Quality of Service ensures voice traffic gets priority over data traffic, preventing call quality issues during busy periods.

- [ ] A **bandwidth capacity plan** documents the number of concurrent calls required and the bandwidth allocated for voice
- [ ] QoS is configured on the **firewall or router** to give VoIP traffic highest priority using DSCP markings (typically EF/46 for voice)
- [ ] QoS is configured on all **network switches** in the voice path to honour DSCP markings and prioritise voice frames
- [ ] A **bandwidth reservation** is configured for voice traffic to guarantee minimum bandwidth even during network saturation
- [ ] Upload bandwidth is specifically assessed — **asymmetric connections** (FTTC) may bottleneck outbound voice traffic before download is affected
- [ ] Call quality testing has been performed during **peak bandwidth usage** (e.g., while running backups, large downloads, or video conferences)
- [ ] A **traffic shaping policy** limits non-essential traffic (streaming, social media) to prevent it consuming bandwidth needed for voice
- [ ] QoS markings are **preserved across the WAN connection** — some ISPs strip DSCP markings at the handover point

Section Score: ____/10

3 Hardware & Handset Inventory

Document all VoIP hardware to ensure compatibility, firmware currency, and adequate spares for the organisation.

- [ ] A complete **inventory of all IP handsets** exists including model, firmware version, MAC address, and assigned extension
- [ ] All handsets are from the **VoIP provider's supported hardware list** — unsupported handsets may lose functionality after platform updates
- [ ] Handset **firmware is current** and provisioned centrally via the VoIP platform's auto-provisioning system
- [ ] **Headsets** used with softphones or desk phones are certified compatible with the VoIP platform (e.g., Jabra, Poly, EPOS)
- [ ] Spare **handsets are available** for rapid replacement — at least 5% of the deployed fleet or a minimum of 2 units
- [ ] Conference room **speakerphones or conference units** are inventoried and tested for audio quality in their installed locations
- [ ] Analogue devices (fax machines, door entry, lift phones) are connected via **Analogue Telephone Adapters (ATAs)** that are documented and monitored
- [ ] Desk phone **power supplies** are via PoE from managed switches — no separate power adapters that could be accidentally disconnected

Section Score: ____/10

4 VoIP Platform Configuration

Verify that the VoIP platform is configured correctly for call routing, voicemail, and business requirements.

- [ ] The **auto-attendant / IVR** is configured with current menu options, correct routing, and a professional greeting
- [ ] **Call routing rules** are documented including business hours, out-of-hours, bank holidays, and emergency overrides
- [ ] Ring groups and **hunt groups** are configured correctly for each department with appropriate ring strategies (simultaneous, sequential)
- [ ] **Voicemail** is configured for all users who require it, with voicemail-to-email delivery verified as working
- [ ] **Call recording** is enabled where required for compliance, training, or quality purposes with appropriate GDPR notices
- [ ] User **presence and status** features are configured and integrated with Microsoft Teams or other collaboration platforms
- [ ] **Music on hold** and transfer announcements are professional, appropriately licensed, and not causing caller frustration
- [ ] All **DDI (Direct Dial-In) numbers** route correctly to the intended extensions, ring groups, or auto-attendants
- [ ] The platform is configured with a **disaster recovery routing plan** that redirects calls to mobiles or an alternative site if the primary system fails

Section Score: _____/10

5 Call Quality Monitoring

Proactive call quality monitoring catches issues before users complain. Reactive troubleshooting is always too late.

- [ ] The VoIP platform provides **call quality metrics** (MOS scores, jitter, latency, packet loss) accessible via an admin dashboard
- [ ] A **Mean Opinion Score (MOS) baseline** has been established — target 4.0 or above for acceptable quality (5.0 is perfect)
- [ ] **Call quality alerts** are configured to notify the IT team when MOS scores drop below acceptable thresholds
- [ ] Call quality is **monitored across all sites** including remote workers, not just the main office
- [ ] Regular **test calls to external numbers** are made to verify inbound and outbound quality from the caller's perspective
- [ ] **Call Detail Records (CDRs)** are retained and reviewed for patterns of dropped calls, short calls, or failed connections
- [ ] A **user feedback mechanism** allows staff to report call quality issues with enough detail to diagnose the problem
- [ ] Network monitoring tools provide **correlation between network events** and call quality degradation for root cause analysis

Section Score: ____/10

6 Security & Compliance

VoIP systems are targets for toll fraud, eavesdropping, and denial-of-service attacks. Protect them accordingly.

- [ ] SIP trunk **authentication credentials** are strong, unique, and changed from any default values
- [ ] **Toll fraud protection** is configured with call barring on premium-rate, international, and high-cost destinations unless explicitly required
- [ ] **SRTP encryption** is enabled for voice media to prevent eavesdropping on calls traversing the network
- [ ] **TLS encryption** is enabled for SIP signalling to protect call setup information and credentials
- [ ] The VoIP platform's **admin interface** is protected with multi-factor authentication and accessible only from trusted networks
- [ ] Voicemail PINs comply with **minimum complexity requirements** and are not set to default values (0000, 1234)
- [ ] **Emergency services (999/112)** are configured correctly with accurate location information transmitted to the emergency operator
- [ ] Call recording and **GDPR compliance** requirements are met with appropriate retention periods and access controls
- [ ] The system is included in regular **security audits and vulnerability assessments**

Section Score: ____ /10

7 Disaster Recovery & Failover

When your VoIP system fails, your business is unreachable. Plan for every failure scenario.

- [ ] A **VoIP disaster recovery plan** is documented covering platform outage, internet failure, power failure, and site unavailability
- [ ] **Call forwarding to mobile phones** is pre-configured and can be activated within minutes of a system failure
- [ ] The VoIP provider offers **geographic redundancy** with automatic failover to a secondary data centre
- [ ] An **internet failover connection** is in place to maintain VoIP service if the primary internet connection fails
- [ ] **UPS (Uninterruptible Power Supply)** protects network switches, routers, and the internet connection to maintain VoIP during short power outages
- [ ] A **softphone application** on mobile devices allows staff to make and receive calls on their business number from anywhere with internet access
- [ ] The DR plan has been **tested within the past 12 months** with documented results and identified improvements
- [ ] Recovery Time Objective (RTO) for **telephony restoration** is defined and achievable with current DR arrangements
- [ ] **Number porting contingency** is understood — if the VoIP provider fails permanently, how quickly can numbers be ported to an alternative

Section Score: _____/10

8 Audit Summary & Action Plan

#	AUDIT AREA	SCORE	PRIORITY
1	Network Infrastructure Assessment	/ 10	H / M / L
2	Bandwidth & QoS Configuration	/ 10	H / M / L
3	Hardware & Handset Inventory	/ 10	H / M / L
4	VoIP Platform Configuration	/ 10	H / M / L
5	Call Quality Monitoring	/ 10	H / M / L
6	Security & Compliance	/ 10	H / M / L
7	Disaster Recovery & Failover	/ 10	H / M / L
TOTAL SCORE		**/ 70**	

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: _____