Secure Communication Readiness Checklist

Use this checklist to evaluate your organization's current communication security maturity and operational readiness.

Check each item that accurately reflects your organisation today.

Email and Communication Security

☐ 1. Employees use strong, unique passwords for communication systems.

☐ 2. Multi-factor authentication (MFA) is enabled for business email accounts.

☐ 3. Employees verify unusual financial or confidential requests independently.

☐ 4. Suspicious attachments and links are treated cautiously.

☐ 5. Communication systems are monitored for unauthorized access activity.

Collaboration and Messaging Governance

☐ 6. Approved communication tools are clearly defined.

☐ 7. Employees understand which messaging platforms are approved for business use.

☐ 8. Access permissions for collaboration tools are reviewed regularly.

☐ 9. External sharing settings are controlled intentionally.

☐ 10. Sensitive discussions use secure communication practices when appropriate.

Confidential Information Protection

☐ 11. Client files and confidential documents are shared through controlled systems.

☐ 12. Employees understand confidentiality expectations across communication platforms.

☐ 13. Cloud storage permissions are reviewed periodically.

☐ 14. Lost or stolen device procedures are clearly defined.

☐ 15. AI tools are governed with clear confidentiality guidance.

Human Awareness and Operational Discipline

☐ 16. Employees receive phishing and social engineering awareness training.

☐ 17. Verification culture is encouraged throughout the organisation.

☐ 18. Employees feel comfortable reporting suspicious communication quickly.

☐ 19. Leadership models secure communication behaviour consistently.

☐ 20. Communication standards remain professional across all platforms.

Remote Work and Incident Preparedness

☐ 21. Remote employees receive guidance on secure communication practices.

☐ 22. Video conferencing security standards are established.

☐ 23. Incident response procedures exist for communication-related compromise.

☐ 24. Backup communication procedures are documented.

☐ 25. Communication policies are reviewed and updated periodically.

SCORING YOUR RESULTS

Strong Maturity: 20–25 Checked Items

Your organisation demonstrates strong communication security awareness and operational discipline.

You likely maintain:

- practical governance,
- employee awareness,
- secure collaboration habits,
- and sustainable communication standards.

Your next step is continuing regular reviews, refining policies, and adapting to evolving communication technologies and threats.

Moderate Exposure: 12–19 Checked Items

Your organisation has implemented some important protections but may still have operational gaps.

Common risks at this level include:

- inconsistent verification habits,
- unmanaged collaboration tools,
- weak remote communication practices,
- or limited AI governance.

Your next step is strengthening communication policies, improving employee awareness, and reviewing access and collaboration controls more consistently.

High Vulnerability: 0–11 Checked Items

Your communication environment may currently create significant operational and cybersecurity exposure.

Risks at this level may include:

- phishing vulnerability,
- unauthorised access,
- insecure file sharing,
- confidentiality breaches,
- and poor incident readiness.

Your next step is establishing foundational communication standards, improving employee awareness, enabling MFA, and reviewing collaboration systems carefully.