Encryption Readiness Audit Checklist

Score each item:

- Yes = 2 points
- Partially = 1 point
- No = 0 points

Foundational Understanding

☐ Leadership understands the difference between password access and actual encrypted unreadability.
☐ We understand the basic distinction between encryption at rest and encryption in transit.
☐ We know which major business systems claim to use encryption and where gaps may still exist.

Devices & Local Storage

☐ Staff laptops and business mobile devices are confirmed to use device encryption.
☐ Sensitive customer or employee files are not routinely stored in unmanaged local folders.
☐ Old USB drives or external backups containing readable data have been reviewed.

File Movement & Sharing

☐ We limit repeated emailing of sensitive readable attachments where possible.
☐ Controlled file sharing methods are preferred over broad public links.
☐ Bulk customer or payroll exports are restricted to necessary personnel.

Staff Handling Behaviour

☐ Employees understand which files count as high-impact sensitive information.
☐ Staff are discouraged from using personal messaging apps for confidential documents.
☐ Employees know not to upload sensitive files into random third-party utility websites.
☐ Sensitive document movement receives more caution than ordinary admin files.

Vendor & SaaS Visibility

☐ We ask providers specifically where data is encrypted and where it becomes readable.
☐ We review local sync behaviour and export practices in cloud systems.
☐ We understand how backups are protected across major vendors.

Archive & Retention Hygiene

☐ Old CRM exports, payroll sheets, and archived readable files are periodically cleaned.
☐ Legacy folders and historic backups are not ignored as harmless storage.

Strategic Readiness

☐ We can identify our highest-value plaintext exposure points today.
☐ We do not assume “our IT handles encryption” without visibility.
☐ Encryption is viewed as part of customer trust and breach reduction — not just technical jargon.

SCORING RESULTS

34–40 Points — STRONG MATURITY

Your organization demonstrates strong practical awareness of how readable data exposure can be reduced through layered encryption discipline.

18–33 Points — MODERATE EXPOSURE

Some encrypted protections likely exist, but staff habits, local copies, or vendor blind spots still create preventable readable-data risk.

0–17 Points — HIGH VULNERABILITY

Your business currently relies heavily on assumption rather than visibility, making sensitive information more readable and exploitable than leadership likely realises.