



## Data Retention Readiness Audit Checklist

Score each item:

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

### Data Visibility

- We understand the major categories of data our business holds.
  - We know which systems and platforms contain duplicate customer or employee records.
  - We have visibility into where old attachments, exports, and cloud archives live.
- 

### Retention Logic

- We can explain why major categories of retained data are still being kept.
  - We do not rely solely on “just in case” thinking for storage decisions.
  - Different data categories have different retention expectations.
- 

### Deletion Discipline

- Routine review and deletion windows exist.
  - Deletion is tied to business events such as offboarding, project closure, or inactivity.
  - Archive does not automatically mean indefinite retention.
- 

### Long-Term Archive Protection

- Sensitive long-retention records have controlled visibility.
- Historic payroll, legal, or tax files are not broadly accessible.
- Backup systems are considered part of retention review.

---

## Legacy Cleanup

- Former employees do not leave behind unmanaged file trails or permissions.
  - Former clients and vendors are not silently accumulating dormant data exposure.
  - Old SaaS platforms are reviewed for lingering records.
- 

## Documentation & Ownership

- Major data families have named review ownership.
  - Retention guidance exists in practical usable form.
  - Review calendars are assigned and recurring.
- 

## Deletion Safety

- Cleanup happens strategically rather than through random panic purges.
  - We understand the difference between deleting one copy and deleting all meaningful copies.
- 

## Strategic Maturity

- Leadership views stored data as an active cyber responsibility, not passive inventory.
  - We understand that unnecessary retained data increases long-term trust and breach burden.
- 

# SCORING RESULTS

## 38–48 Points — STRONG MATURITY

Your organization demonstrates healthy data lifecycle awareness, reduced stale liability, and stronger long-term cyber governance.

## 20–37 Points — MODERATE EXPOSURE

Some retention awareness exists, but data accumulation and inconsistent cleanup still create avoidable cyber burden.

## **0–19 Points — HIGH VULNERABILITY**

Your business is likely storing large volumes of unmanaged stale data that continue to create exposure without proportional operational value.