



Security Culture Readiness Assessment Checklist

Instructions

Use this checklist to evaluate your organisation's cybersecurity awareness maturity and operational resilience culture.

Score each item:

- Yes = 2 points
- Partial/In Progress = 1 point
- No = 0 points

Leadership & Governance

- Leadership visibly supports cybersecurity awareness initiatives.
- Cybersecurity awareness is treated as an operational priority.
- Governance reporting includes human risk visibility.
- Managers reinforce awareness expectations consistently.
- Operational policies are communicated clearly.

Employee Awareness & Engagement

- Employees receive ongoing cybersecurity awareness training.
 - Phishing awareness exercises occur regularly.
 - Awareness content is practical and operationally relevant.
 - Employees understand reporting procedures.
 - Workforce engagement with awareness initiatives is strong.
-

Reporting Culture & Communication

- Employees feel comfortable reporting suspicious activity.
 - Reporting procedures are simple and clearly documented.
 - Operational transparency is encouraged.
 - Blame-focused culture is actively discouraged.
 - Incident escalation processes are operationally understood.
-

Operational Discipline & Remote Work Security

- MFA is widely adopted across the organization.
 - Employees follow secure password practices.
 - Remote workforce security guidance exists.
 - Device management expectations are reinforced.
 - Collaboration platform awareness is included in training.
-

Long-Term Resilience & Continuous Improvement

- Awareness programs are reviewed continuously.
 - Leadership participates in awareness communication.
 - Human risk metrics are tracked operationally.
 - Security culture improvements are part of long-term planning.
 - Awareness initiatives adapt to emerging threats.
-

Scoring Results

40–50 Points — Strong Security Culture Maturity

Your organisation demonstrates strong awareness culture, operational discipline, and resilience-focused governance.

Continue strengthening:

- employee engagement,
 - operational visibility,
 - and continuous awareness improvement.
-

20–39 Points — Moderate Human Risk Exposure

Your organisation has foundational awareness practices but may still face:

- inconsistent reporting culture,
- operational gaps,
- or limited awareness engagement.

Focus on:

- leadership visibility,
 - reporting culture,
 - continuous learning,
 - and operational consistency.
-

0–19 Points — High Organisational Vulnerability

Your organisation may face significant exposure involving:

- weak awareness culture,
- poor reporting behaviour,
- inconsistent operational discipline,
- or limited governance visibility.

Immediate priorities should include:

- leadership engagement,
- awareness program improvement,
- reporting culture development,

and operational communication strengthening.