IT MATURITY & BUSINESS REVIEWS

IT maturity assessment.

Give leadership a clear account of the controls and practices supported by your current evidence. Use that baseline to agree priorities, ownership and the next review.

HOW IT WORKS

1. **Agree the questions and boundary.**
   Decide what leadership needs to decide, then confirm the connected sources and the areas in scope for the review.
2. **Bring the evidence together.**
   Combine supported identity, device, network, vulnerability and awareness signals with recorded programme context.
3. **Assess control coverage.**
   Separate a control that is operating, one only partly applied, an observed gap and an area the current collection cannot assess.
4. **Brief and prioritise.**
   Produce a business review and leadership briefing that connects findings to funding, ownership and accepted-risk decisions.
5. **Review with fresh evidence.**
   At the next review, compare scope and evidence freshness as well as findings, so progress reflects verified change.

WHAT THE MATURITY ASSESSMENT CAN DISTINGUISH

- Controls that are operating with supporting evidence, from those that are only partly applied.
- Observed gaps that need remediation, from areas the current collection cannot assess.
- Identity, device, endpoint-protection and vulnerability posture across the estate.
- Network-security and security-awareness signals where those sources are connected.
- Recorded risks, approved policies and roadmap items that add programme context.
- Change between reviews driven by verified work, not only by a moved score or a closed ticket.

The view is directional and follows the controls and signals implemented in the platform. It does not assess every framework requirement, and a framework label is not evidence that a control is effective.

Framework alignment. The maturity model uses selected CIS-aligned control references and NIST Cyber Security Framework perspectives to organise the discussion, and it can be read alongside the themes of a UK Cyber Essentials review. This gives leadership and technical teams a shared, framework-anchored baseline to work from.

Start with an authorised, read-only scope

Begin with your assessment questions; we agree coverage and delivery before any commitment.

threatshield@threatshield.global

Read the full page ↗

ThreatShield is part of ITS Consulting — ITS Consulting Ltd (United Kingdom) and ITS Consulting LLC (United States). This guide summarises an assessment capability; the actual scope, coverage and evidence available depend on your environment, licensing and permissions. Framework references organise findings and are not a certification or an assurance that a control is effective. © 2026 ThreatShield.