

ITogether Service Definition Document – Cyber Health Check

Detailed Description

The ITogether Cyber Health Check is a structured assessment designed to provide organisations with a clear, independent view of their current cyber security posture. It focuses on identifying gaps, weaknesses and misalignments between existing controls, real-world threats and operational risk.

The service combines technical review with governance and process analysis. It examines people, process and technology across key cyber security domains, without assuming a specific vendor or solution.

The outcome is a practical, prioritised set of findings that senior IT and business stakeholders can use to inform decision-making, investment planning and risk discussions with the board.

The Cyber Health Check is suitable for organisations of all sizes and maturity levels, including those with limited internal cyber capability or those seeking validation of existing controls.

Business Benefits

- Clear visibility of cyber risk based on real-world exposure, not assumptions
- Independent assessment with no vendor bias
- Identification of quick wins and priority remediation areas
- Improved ability to justify cyber investment and budgets
- Better alignment between technical controls and business risk
- Stronger narrative for board-level and audit discussions
- Baseline view to support future cyber strategy or roadmap development

In real-world environments, organisations often discover that existing tools are underutilised or misconfigured. Addressing these gaps frequently delivers measurable risk reduction without additional spend.

Standard Service Components



The information in this document is the property of Network Integration Technologies Ltd t/a ITogether. The contents of this document must not be reproduced or disclosed wholly or in part or used for purposes other than that for which it is supplied without the prior written permission of Network Integration Technologies Ltd t/a ITogether.

Standard Service Components

- Discovery and scoping workshop with key stakeholders
- Review of existing cyber policies, standards and procedures
- Assessment of identity, access and privilege management
- Review of endpoint, network and perimeter security controls
- High-level review of monitoring, logging and incident response readiness
- Evaluation of user awareness and human risk factors
- Alignment review against recognised frameworks (e.g. NCSC, Cyber Essentials, ISO 27001 principles)
- Risk-based findings with business impact explained in plain language
- Prioritised recommendations and next steps report

Optional Service Components

To be discussed during scoping exercise.

Service Exclusions

Anything not specifically included in either the above or when the project is formally scoped.

Standard Support Services

8x5 support, Monday to Friday 9am to 5pm

Assumptions

Any and all information will be provided by the customer to enable the full onboarding of the product without hinderance

Contact

Name	Role	Tel	Email
Tim Ripper	Account Director	0113 341 0123	tim@itogether.co.uk
Simon Richardson	Director	0113 341 0123	simon@itogether.co.uk



The information in this document is the property of Network Integration Technologies Ltd t/a ITogether.
The contents of this document must not be reproduced or disclosed wholly or in part or used for purposes other than that for which it is supplied without the prior written permission of Network Integration Technologies Ltd t/a ITogether.