ITogether Service Definition Document – Managed Security Awareness & Human Risk Management

Detailed Description
Managed Security Awareness & Human Risk Management is a fully managed service that helps organisations reduce cyber risk caused by human behaviour. The service focuses on building safer habits, improving decision-making, and reducing the likelihood and impact of user-led security incidents such as phishing, credential compromise, and data loss. The service combines ongoing user education, simulated attacks, behavioural analytics, and risk-based reporting. It moves beyond traditional "tick-box" training by measuring how people actually behave and targeting support where risk is highest. Delivered by experienced cyber security professionals, the service includes the design, delivery, and continuous improvement of an awareness programme aligned to organisational risk, regulatory expectations, and public sector assurance requirements. Content and campaigns are adapted over time to reflect emerging threats and changes in user behaviour. The service supports organisations of all sizes and can be aligned to common public sector frameworks and standards. It complements technical security controls by addressing the human element of cyber security, which remains a primary cause of security incidents.

Business Benefits
Reduced human-led cyber risk • Lower likelihood of successful phishing, social engineering, and credential theft. • Improved user decision-making in real-world scenarios. **Measurable improvement** • Clear metrics showing changes in behaviour over time. • Risk-based reporting rather than simple course completion rates. **Targeted and relevant training** • Campaigns tailored to user roles, risk profiles, and behaviours. • Focus on high-risk users and activities.

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.

Improved compliance and assurance

- Supports alignment with public sector standards and audit expectations.
- Evidence-based reporting for governance and risk committees.

Reduced burden on internal teams

- Day-to-day management handled by specialists.
- No requirement to design, run, or analyse campaigns internally.

Cultural change, not box-ticking

- Ongoing engagement rather than annual training.
- Reinforces secure behaviour as part of day-to-day work.

Standard Service Components

Programme design and onboarding

- Review of organisational risk, user groups, and existing training.
- Definition of objectives, success metrics, and reporting requirements.
- Alignment with organisational policies and standards.

Security awareness training

- Delivery of role-based and risk-based training content.
- Ongoing refresh of material to reflect current threats.
- Support for induction and refresher training.

Phishing and social engineering simulations

- Regular simulated phishing campaigns.
- Scenarios aligned to real-world attack techniques.
- Safe handling and support for users who fail simulations.

Human risk measurement

- Behavioural data analysis to identify high-risk patterns.
- Tracking of trends such as click rates, reporting rates, and repeat failures.
- Risk scoring to prioritise interventions.

Targeted interventions

- Additional training or coaching for higher-risk users.
- Just-in-time education following risky actions.
- Adaptive campaigns based on observed behaviour.

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.

Reporting and service reviews

- Regular reports covering engagement, risk trends, and progress.
- Executive-level summaries for senior stakeholders.
- Recommendations for improving outcomes.

Service governance and support

- Defined service levels and support processes.
- Ongoing programme management and optimisation.
- Coordination with customer security and IT teams.

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.