ITogether Service Definition Document – Managed Network & Cyber Security Operations

Detailed Description
Managed Network & Cyber Security Operations provides the day-to-day operational management of network and cyber security controls to maintain availability, resilience, and protection against evolving threats. The service integrates network operations and cyber security operations to provide coordinated monitoring, incident response, and continuous improvement. The service covers ongoing oversight of network infrastructure, security platforms, and supporting processes across on-premise, cloud, and hybrid environments. It focuses on early detection of incidents, effective response, and reducing operational and security risk. Delivered by experienced network and cyber security specialists, the service removes the burden of running complex operational functions internally. It provides structured processes, defined service levels, and clear accountability while supporting collaboration with internal IT, security, and risk teams. Managed Network & Cyber Security Operations is suitable for public sector organisations that require reliable connectivity and robust security controls to support critical services, staff, and users.

Business Benefits
Improved resilience and availability o Coordinated management of network and security incidents. o Reduced downtime and service disruption. **Reduced cyber and operational risk** o Continuous monitoring and rapid response to threats and faults. o Consistent application of security and network controls. **Operational efficiency** o Day-to-day operations managed by an external service. o Internal teams focus on strategy, transformation, and improvement.

Access to specialist capability

- Experienced engineers across network and cyber security domains.
- Support for complex, multi-vendor environments.

Improved visibility and assurance

- Clear insight into incidents, trends, and risks.
- Reporting to support governance, audit, and senior stakeholders.

Scalable and adaptable

- Service scales with organisational growth and change.
- Supports evolving architectures and threat landscapes.

Standard Service Components

Service onboarding and discovery

- Review of network and security architecture and services.
- Identification of critical systems, dependencies, and risks.
- Agreement of scope, responsibilities, and escalation paths.

Integrated monitoring and operations

- Continuous monitoring of network and security platforms.
- Detection of faults, threats, and abnormal behaviour.
- Coordinated response across network and security domains.

Incident management and response

- Triage and investigation of incidents.
- Containment, remediation, and recovery support.
- Coordination with customer teams and third parties.

Security operations support

- Oversight of security alerts and events.
- Support for threat investigation and response.
- Alignment with organisational security policies.

Network operations support

- Monitoring of performance, capacity, and availability.
- Identification of underlying or recurring issues.
- Recommendations for improvement and optimisation.

Reporting and service reviews

- Regular operational and security reporting.
- Trend analysis and risk insights.
- Scheduled service review meetings.

Service governance and support

- Defined service levels and operational processes.
- Clear communication and escalation routes.
- Alignment with public sector operational and assurance requirements.

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