ITSUS Consulting

G-Cloud 15
Service Definition Document

Commercial-in-Confidence

CONTENTS

- Capability Areas
- Purpose, Values & Behaviours
- Supplier Accreditations
- Security Partner of Choice
- Service Lifecycle & Planning
- Support Levels
- SLA Table
- ICT Discovery & Audit Service
- Security Assessment & Discovery Service
- Breach Attack Simulation Service
- Co-Managed Firewall Service
- Training Service
- Corporate Social Responsibility

SECURE COMMUNICATIONS EXPERTLY DELIVERED

CAPABILITY AREAS

ITSUS is a specialist networks and cyber security SME, providing a wide range of ICT lifecycle services to defence and public sector for twenty years. Our approach to successful service delivery is through building long term relationships, focusing on collaboration with our customer, their partners and suppliers, to deliver successful outcomes.

We have partnerships with a variety of world leading ICT vendors including Cisco, Dell, Elastic, Fortinet, Keysight, Microsoft, Palo Alto Networks, SolarWinds and VMware with consultants experienced and qualified across a wide variety of project delivery methodologies and technology.

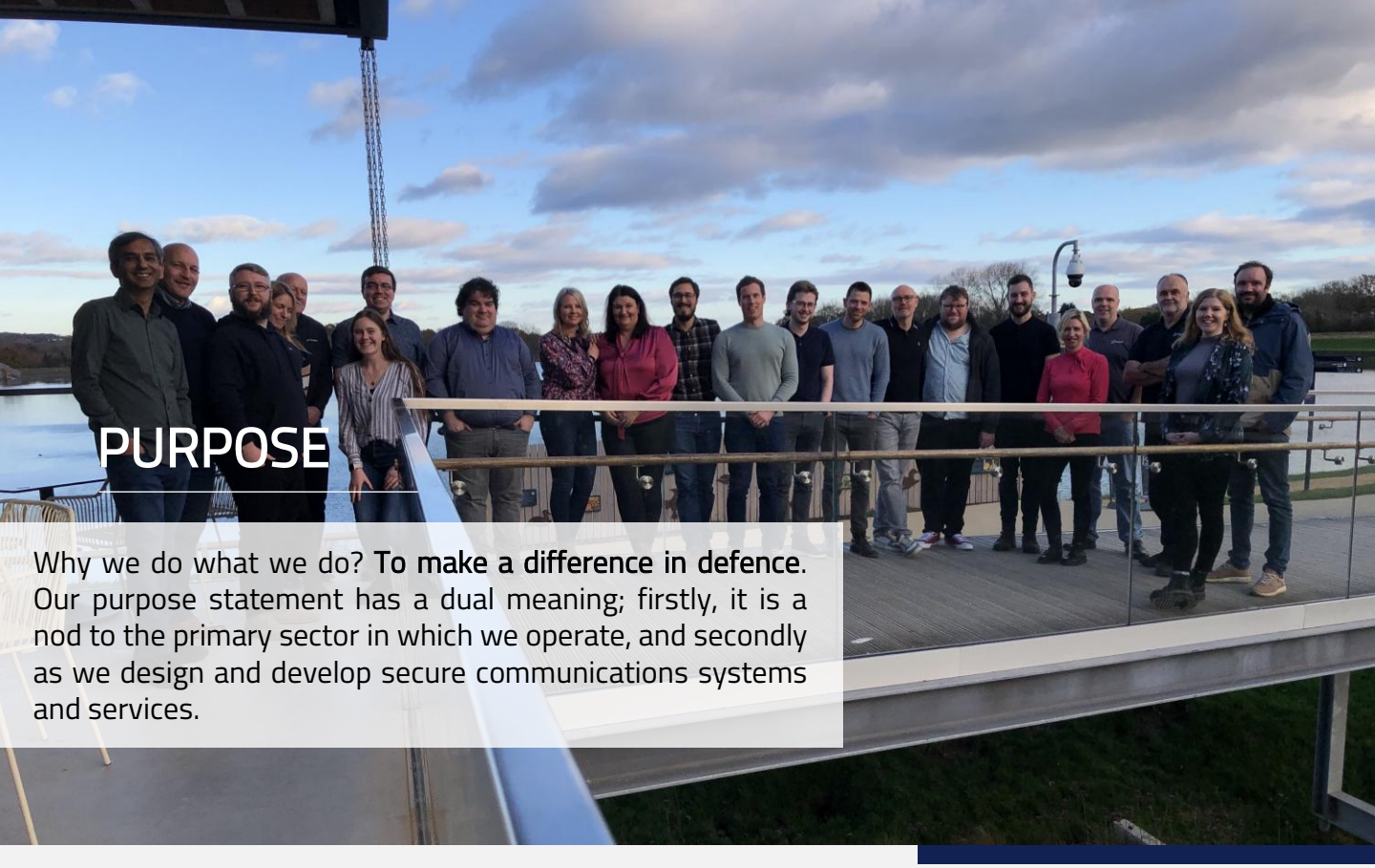
Networks

Cyber Security

Data Science

Security is very much at the core of our delivery and our company is a validated cyber security supplier to HMG, we are ISO 27001 accredited, and all staff are UK MOD security cleared. With our growing highly skilled multi-disciplinary team, we continue to expand and evolve our broad capabilities in line with market demand. This adaptability has garnered us a firm reputation within defence and government, allowing us to expand our scope, from networks and infrastructure to the evolving fields of cyber security and data science.

ITSUS CONSULTING



PURPOSE

Why we do what we do? **To make a difference in defence**. Our purpose statement has a dual meaning; firstly, it is a nod to the primary sector in which we operate, and secondly as we design and develop secure communications systems and services.

VALUES & BEHAVIOURS

Our company values are shared across our team:

Ambition – Achieving success through our people
Collaboration – Open-minded, agile, committed
Excellence – Secure communications expertly delivered

Our purpose is supported by our core behaviours and upheld by the wider team to a high standard:

Adaptable – Remain agile and in tune to customer needs
Responsive – Maintain effective communication
Committed – Building long-lasting relationships

ITSUS CONSULTING

ACCREDITATIONS

- Cyber Essentials
- Cyber Essentials Plus
- Defence ERS Silver Award
- ISO 9001:2015
- ISO 27001:2022
- Pension Quality Mark (PQM)

MEMBERSHIPS

- ADS Group
- Cyber Wales
- NCSC CyberFirst
- Women Empowering Defence (WED)

TECHNOLOGY PARTNERSHIPS

- Cisco Premier Partner
- Dell
- Elastic
- Fortinet
- Keysight Technologies
- Microsoft
- Palo Alto Networks
- Solar Winds
- VMware
- 4Secure

SUPPLY CHAIN

- Crown Commercial Service (CCS)
- HMG Cyber Security Supplier
- JOSCAR ID: JSAR01001052
- NATO NCAGE Code: U19C6
- Team Tempest Approved Supplier

SECURITY PARTNER OF CHOICE

ITSUS is the network security partner of choice due to our expertise, collaborative ethos, and proven ability to secure mission-critical environments. We deliver network and cyber security services to aerospace, defence, and public-sector organisations through repeatable, proven service approaches that deliver resilience while aligning to each customer's operational needs. Our collaborative approach gives customers clear insight and visibility, supported by ICT experts whose purpose is to promote challenge and foster continuous improvement. Operating deeply within the UK defence ecosystem, we support sensitive programmes requiring trusted delivery and appropriate national-security vetting. With the UK's Cyber Security and Resilience Bill strengthening regulatory expectations, our G-Cloud 15 services offer timely, compliant, and future-ready security capabilities for public-sector organisations.

G-CLOUD 15 ROLES

- Architecture
- IT Operations
- Chief Digital & Data
- Quality Assurance & Testing
- Cyber Security
- Software Development

SERVICE LIFECYCLE

ITSUS delivers a broad range of multi-cloud and on-premises technical support services across defence and public sector environments. Our highly skilled and MOD-security-cleared professionals support customers at all stages of the service lifecycle; from ICT discovery and assessment activities, through to the co-management of complex firewall estates. We also provide comprehensive training and knowledge transfer, ensuring customer teams remain confident, capable, and empowered long after the service is delivered.

SERVICE PLANNING

At ITSUS, successful delivery begins with thorough and considered planning. Our approach centres on regular stakeholder engagement and open communication to ensure alignment from the outset. We deploy a highly skilled and experienced team who bring the right attitudes and professional behaviours to every engagement, fostering trust and collaboration. By delivering early insights and maintaining transparent, iterative updates, we keep customers informed and confident throughout the process. Our defined ways of working—including secure information sharing and controlled disclosure—provide structure, rigour, and assurance across each stage of the service lifecycle, enabling consistently high-quality outcomes.

SUPPORT LEVELS

Three operational support levels (L1, L2, L3), with optional L4 architecture, strategy and governance support. All cloud and on-premise support services are overseen by a highly experienced Technical Account Manager.

★

Level 1 — Intake, Triage & Coordination

- Single point of contact for all services
- Handles request validation, ticket creation and prioritisation
- Performs basic health checks
- Coordinates with customer teams and escalates to L2/L3
- 09:00–17:00 operational support

★★

Level 2 — Technical Analysts / Security Analysts

- Performs routine firewall changes, rule hygiene and log checks
- Supports evidence collection for assessments
- Assists in BAS planning and preparation
- Initial technical troubleshooting
- Validates data, review findings and prepares customer updates

★★★

Level 3 — Senior Network Security Engineers

- Advanced firewall and network engineering
- Leads security assessments, interprets findings, and provides recommendations
- Conducts BAS scenario design, runs high-complexity tests and analyses attack paths
- Root-cause analysis and complex troubleshooting
- Vendor liaison (e.g., Cisco & Palo Alto TAC)

★★★★

Level 4 (OPTIONAL) — Architecture, Strategy & Governance

- Security architecture and roadmap
- Multi-cloud design reviews
- Strategic risk management
- Oversight of BAS outcomes and reduction plans
- Policy frameworks and governance

SLA TABLE

Category	SLA Type	Definition	Response Time	Notes
Incidents – Critical	P1	Service-impacting firewall outage or major security event	1 hour	Clock runs from 09:00–17:00
Incidents – High	P2	Significant firewall degradation or urgent security alert	1 hour	L2/L3 engaged quickly
Incidents – Medium	P3	Non-critical performance issues or routine alerts	4 hours	
Incidents – Low	P4	Minor issues	Next business day	
Standard Firewall Change	Change	Pre-approved low-risk change (rules, NAT, objects)	1–2 business days	
Complex Firewall Change	Change	High-complexity change requiring senior review	3–5 business days	
Emergency Firewall Change	Change	Required to address critical risk/outage	1 hour	Requires justification
Security Assessment – Queries	Assessment	Information requests, artefacts and clarifications	1 business day	Keeps assessment on track
Security Assessment – Findings Review	Assessment	Follow-up discussion on draft findings	1 business day	Supports early-insights model
BAS – Execution Queries	BAS	Questions during live BAS scenario	4 hours	Within 09:00–17:00
BAS – Reporting Queries	BAS	Clarifications on attack paths and results	1 business day	
ICT Audit & Discovery – Information Requests	Audit	Artefact requests, clarifications and SME follow-ups	1 business day	Typical for discovery cycles
ICT Audit & Discovery – Early Insights Review	Audit	Discussion of preliminary findings/themes	1 business day	Enables collaborative validation
Training Services – Scheduling Queries	Training	Questions about course dates, availability and logistics	2 business days	Depends on trainer schedules
Training Services – Learner Support Requests	Training	Follow-up questions, lab access issues and material clarifications	1 business day	Supports smooth learner experience

ICT DISCOVERY & AUDIT SERVICE

Service Description: ICT discovery and audit service providing a comprehensive assessment of ICT, network and security environments. We identify vulnerabilities, inefficiencies and improvement opportunities, delivering evidence-based insights and clear recommendations. Often the first step in digital transformation, risk reduction and improving performance, resilience and compliance across complex ICT estates.

Service Constraints: Delivery depends on access to relevant documentation, systems, configurations and stakeholder availability. Assessment findings are based on the agreed scope and discovery period and do not constitute continuous monitoring. Some recommendations may require additional analysis or follow-on services to implement. Access to sensitive systems is subject to customer approval and security policies. Timelines may vary depending on estate size, complexity and data availability. All information collected is handled securely and treated as confidential.

Features:

- Full ICT, network and security estate discovery
- Independent configuration, controls and process audit
- Vulnerability, misconfiguration and technical-debt identification
- Performance, reliability and resilience assessment
- Policy, standards and compliance review
- Firewall and network architecture analysis
- Workshops and structured stakeholder information gathering
- Cloud, hybrid and on-prem environment coverage
- Executive summaries and detailed technical reporting
- Prioritised improvement roadmap with timelines

Benefits:

- Stronger, evidence-based ICT decision-making
- Reduced operational and security risk
- Improved network performance and reliability
- Greater visibility across complex environments
- Clear understanding of configuration weaknesses
- Enhanced compliance and audit readiness
- Better alignment with industry best practice
- Informed planning for digital transformation
- Increased assurance across hybrid estates
- Practical, actionable recommendations

SECURITY ASSESSMENT & DISCOVERY SERVICE

Service Description: The security assessment and discovery service provides deep visibility into network activity, applications, threats and vulnerabilities. Using tool-assisted discovery and industry benchmarks, we assess security posture, identify risks and misconfigurations, and deliver clear, prioritised remediation roadmaps. Enables informed decision-making, improved resilience and stronger alignment with security best practice.

Service Constraints: The security assessment and discovery service operates using passive data collection only, meaning visibility is dependent on the availability and quality of existing logs, traffic flow data and system configurations. Findings rely on the customer providing timely access to required artefacts, network visibility points and subject-matter experts. Assessments do not include intrusive testing, configuration changes or live exploitation activities. Cloud, hybrid and on-premises coverage may vary depending on deployed tooling and permissions. Remediation actions identified are advisory and require customer approval and implementation. Accuracy of results may be limited where encrypted traffic cannot be decrypted or monitored.

Features:

- Deep network, application and threat visibility
- Industry-standard security posture benchmarking
- Vulnerability, misconfiguration and technical-debt identification
- SSL decryption and encrypted-traffic risk assessment
- Policy and rule-set hygiene review
- Risk analysis to reduce attack surface
- Executive-ready technical and strategic reporting
- Passive assessment with zero production impact
- C2 beaconing and malware behaviour detection
- Coverage for on-prem, cloud and hybrid environments

Benefits:

- Improved organisational security posture
- Reduced attack surface and exposure
- Confident, data-driven security decisions
- Better visibility and application control
- Enhanced accountability for user activity
- Early detection of emerging and zero-day threats
- Optimised firewall and access policies
- Strengthened compliance and audit alignment
- Increased assurance across hybrid environments
- Clear, prioritised remediation actions

BREACH ATTACK & SIMULATION SERVICE

Service Description: Continuous breach and attack simulation service that safely emulates real attacker behaviours across the cyber kill chain to validate security controls. Provides fast visibility, automated validation, prioritised remediation and measurable exposure reduction. Co-managed with your teams to improve resilience, compliance and security posture month by month.

Service Constraints: Simulations use isolated test endpoints only and never affect production systems or user devices. Test frequency varies based on customer change cycles, environment size and coverage. Remediation can be added as a service but may require approvals, access or maintenance windows. Integrations with ticketing, SIEM or EDR platforms depend on customer permissions. Some high-risk scenarios need prior agreement. Services run during UK business hours unless enhanced support is agreed. Customers must ensure stable network connectivity for scheduling and reporting.

Features:

- Safe, automated breach and attack simulation across live defences
- MITRE ATT&CK-aligned scenarios across the full kill chain
- Change-triggered and scheduled test cadence
- Isolated test endpoints; no production impact
- Prioritised remediation guidance with step-by-step actions
- Exposure scoring, KPI trends and executive reporting
- Integrates with ticketing; supports DevOps workflows
- Compliance reporting and audit-ready evidence packs
- Realistic phishing, ransomware, C2 and lateral movement suites
- On-prem, cloud and remote coverage

Benefits:

- Improve security posture month by month
- Measurable improvements to MTTD and MTTR
- Fewer incidents after change windows
- Confident, data-driven security decisions
- Proves controls work against real TTPs
- Accelerates remediation; focuses on highest risks
- Board-ready KPI deltas and summaries
- Regulatory and audit confidence
- Enhanced resilience across hybrid environments
- Co-managed improvements aligned with your teams

CO-MANAGED FIREWALL SERVICE

Service Description: Managed firewall service providing secure, co-managed operation of cloud, on-premises and hybrid firewall estates. We manage configuration, patching, upgrades and day-to-day operations, delivering visibility, continuous improvement and reduced risk. Includes onboarding audit, ongoing reviews, executive reporting and alignment with your security strategy.

Service Constraints: Service delivery depends on agreed onboarding, scope definition and secure remote access to firewall platforms. Supported activities are limited to the technologies and assets defined in the service scope and RACI. Change volumes and out-of-hours activities may be subject to additional charges. Updates or configuration changes may be constrained by operational criticality, maintenance windows or regulatory requirements. Monitoring and management rely on stable connectivity between customer environments and the ITSUS Managed Service Centre. On-site support is not included unless separately agreed.

Features:

- Co-managed NGFW configuration, policy updates and change control
- Patch, firmware, antivirus and malware update management
- Threat prevention and secure remote access support
- VPN configuration, optimisation and lifecycle management
- AI-Ops-driven device health and predictive maintenance
- Custom dashboards and real-time estate visibility
- Quarterly Security Lifecycle Reviews with action plans
- Cloud, on-prem and hybrid firewall estate coverage
- Expert triage and escalation to vendors
- Continuous ruleset hygiene and configuration optimisation

Benefits:

- Stronger, continuously improving security posture
- Reduced misconfigurations and policy drift
- Improved uptime and operational stability
- Faster incident response and troubleshooting
- Clear visibility of firewall performance and risks
- Better utilisation of existing security investments
- Reduced internal workload and operational burden
- Increased compliance readiness and audit assurance
- Scalable management across hybrid environments
- Confidence through expert, proactive oversight

TRAINING SERVICE

Service Description: Bespoke technical and cybersecurity training covering vendor technologies, CyBOK and NCSC table-top exercises, software and systems training, operational procedure documentation and cyber leadership development. Delivered by experienced practitioners and academics, our programmes improve skills, reduce security risk and enhance organisational capability through hands-on, scenario-based learning.

Service Constraints: Training delivery requires suitable facilities for workshops, table-top exercises or hands-on labs, whether onsite or remote. Some technical courses may require access to customer systems, sandbox environments or specific vendor tools. Custom programme design depends on timely access to subject matter experts and operational documentation. Remote sessions rely on stable connectivity and agreed collaboration platforms. Scheduling availability may be influenced by customer operational cycles, change windows or security restrictions. Certain advanced modules may require prerequisite knowledge or role-based access privileges.

Features:

- Vendor-specific technical training across networks, cyber and platforms
- CyBOK and NCSC-aligned cybersecurity table-top exercises
- Hands-on practical labs and guided workshops
- Bespoke user and system-specific training programmes
- Cyber leadership and organisational resilience training
- Customised curricula for varied learning styles
- Post-training resources for continued development
- Role-focused skills uplift for technical teams
- Cloud, infrastructure and security fundamentals training
- Delivered by practitioners, engineers and academic specialists

Benefits:

- Stronger cyber awareness and behavioural resilience
- Improved technical capability across ICT teams
- Enhanced operational readiness and confidence
- Better value from existing technology investments
- Reduced risk through informed, capable staff
- Improved compliance and audit alignment
- Accelerated onboarding of new team members
- Increased staff retention through professional development
- Consistent knowledge across hybrid environments
- Clear, measurable uplift in team capability

CORPORATE SOCIAL RESPONSIBILITY

Our social values reflect our vision to support and grow a diverse team. This involves supporting and being a part of communities that are important to us; sponsoring local junior and senior sports teams, participating as a member of the NCSC's CyberFirst programme, being a signatory of the Armed Forces Covenant, being an inaugural member of Cyber Wales, a member of ADS Group, and fostering close relationships with several local universities.

COMMUNITY ENGAGEMENT

Marc, former Llanishen RFC 2nd team captain, continues to serve on the club committee.

"It means a lot for ITSUS to be supporting our very local community through sport and the social engagement of Llanishen RFC."

Marc Williams | Senior Network Engineer

Shahid coaches two different age groups in Lisvane Panthers FC, one of the largest football clubs in Wales.

"I'm really passionate about grassroots sport and developing a team ethic at an early age. We're also proud to sponsor a local South Wales U14s football team."

Dr Shahid Mian | Managing Director

Clare is part of the team behind the BSides Cymru community and is the founder of the Women in Cyber Wales network.

"Building strong relationships with the wider community is something I feel really strongly about. It enables us to connect with people in a really positive way."

Dr Clare Johnson | Networks & Cyber Capability Lead

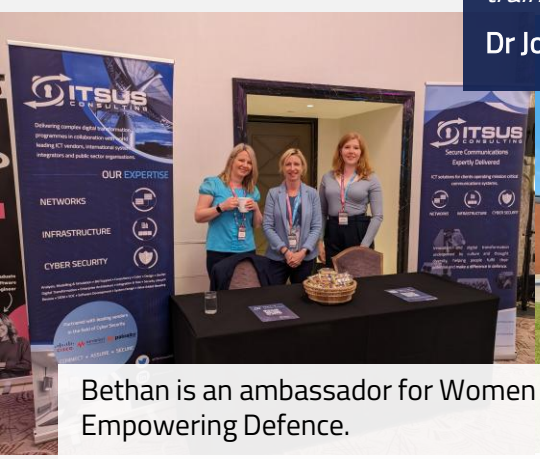
ACADEMIA & INDUSTRY

We regularly engage with local academia and communities in our industry and encourage our team to be active in the groups they draw value from. Our engagements allow us to form strong partnerships and develop a better understanding of what we can do to support the communities we work with.

Jon joined ITSUS from a lectureship position at Swansea University.

"Our relationships with the universities in South Wales allows us to regularly engage with a pool of highly-skilled minds, and shape the programmes for training future doctoral candidates."

Dr Jonathan-Lee Jones | Senior Research Technologist



Bethan is an ambassador for Women Empowering Defence.

"Supporting underrepresented groups within the defence industry like WED helps break down the barriers to entry and foster a sense of inclusion."

Bethan Davies | Marketing Executive

Holly heads the team's personal development plans and looks to industry standards to understand how best to guide the team.

"Our ADS membership is a great resource that helps keep us abreast of complex and often changing industry needs."

Holly Barnes | Operations Manager

ITSUS Consulting Ltd
4 Cwrt Y Parc, Cardiff CF14 5GH
Company No. 06628075

Website
www.itsusconsulting.com
ITSUS Consulting
4 Earlswood Road, Cardiff CF14 5GH
Phone
02920 003 170
Email
sales@itsusconsulting.com