



Cybersecurity Strategy, Assurance and Readiness
Service Definition Document | G-Cloud 15 | Lot 3

morson PRAXIS

Cybersecurity Strategy, Assurance and Readiness

Through strategy-led digital transformation, Morson Praxis helps public sector organisations to accelerate benefits realisation, reimagine operations, enable scalable innovation and build resilience for the future. We ensure that every technological investment, from large-scale enterprise transformation to focused project delivery, creates sustainable, meaningful change.

Service Definition for Cybersecurity Strategy, Assurance and Readiness

Morson Praxis's Cybersecurity Strategy, Assurance & Readiness service supports organisations in understanding whether their cybersecurity approach is fit for purpose before, during, or alongside digital delivery. The service is designed for organisations that require confidence in cyber risk management, governance, and readiness without transferring operational security responsibility.

The service focuses on assessing cybersecurity strategy, governance, risk management, and organisational readiness across digital, data, and cloud-enabled services. We provide an independent, evidence-based view of how cyber risk is understood, governed, and managed, identifying material risks and assurance gaps that could impact delivery outcomes, regulatory compliance, or organisational resilience.

The service is typically used during discovery or pre-delivery phases, ahead of major change or cloud adoption, or as part of assurance, reset, or audit preparation activity.

1. What the service includes

The service typically includes:

- Review and assessment of cybersecurity strategy and direction
- Assessment of cybersecurity governance, ownership, and accountability
- Alignment of cyber risk management with organisational risk appetite
- High-level assessment of cyber risk and control effectiveness
- Alignment with recognised standards and guidance (e.g. NCSC, ISO 27001)
- Assessment of security readiness for cloud, data, and digital services
- Review of data protection, privacy, and information security considerations
- Assessment of organisational cyber capability, culture, and awareness
- Review of incident management readiness at a governance level
- Independent identification of material cyber risks and assurance gaps
- Clear, prioritised recommendations to strengthen cybersecurity readiness

2. What the service does not include

The service does not include:

- Penetration testing or vulnerability scanning
- Technical security testing or red teaming

- Design or implementation of security architectures or controls
- Configuration or deployment of security tools or platforms
- Security operations centre (SOC) services
- Incident response execution or forensic investigation
- Ongoing security monitoring or managed security services

These activities are outside the scope of this service and, where required, may be delivered through separate services procured under the appropriate G-Cloud lots or through alternative procurement routes.

3. How the service is delivered

The service is delivered through a structured, time-bound engagement combining desktop review, stakeholder interviews, and facilitated assessment workshops. Delivery is proportionate to organisational size, complexity, and risk profile, ensuring findings are focused, pragmatic, and actionable.

The approach is independent and evidence-led, providing objective insight into how cybersecurity operates in practice, including governance effectiveness, decision-making, and readiness to manage cyber risk during change. Findings are validated with senior stakeholders to ensure accuracy, shared understanding, and alignment on priorities for action.

The service is technology-agnostic and avoids premature commitment to tools, platforms, or delivery models.

4. Roles and responsibilities

Morson Praxis is responsible for:

- Leading cybersecurity strategy, assurance, and readiness assessment activities
- Conducting independent analysis of cyber risk and governance arrangements
- Facilitating stakeholder engagement and assessment workshops
- Developing structured findings and recommendations
- Providing objective advice to senior leaders and risk owners

The Buyer is responsible for:

- Providing access to relevant stakeholders and documentation
- Supporting engagement across digital, data, risk, and security functions
- Reviewing and validating findings and recommendations
- Retaining ownership of cyber risk decisions and outcomes

5. Service outputs and deliverables

Typical outputs may include:

- Cybersecurity strategy, assurance, and readiness assessment summary
- Identification of material cyber risks and assurance gaps
- Governance and accountability findings
- Prioritised recommendations to improve cyber readiness
- Inputs to audit, assurance, or programme governance activity

Deliverables are tailored to Buyer needs and agreed at the outset.

6. Dependencies and prerequisites

Effective delivery of this service typically depends on:

- Access to cybersecurity, risk, and delivery stakeholders
- Availability of existing security policies, standards, and documentation
- Willingness to engage openly on cyber risk and constraints
- Appropriate sponsorship to act on assurance findings

7. Alignment with G-Cloud 15 Lot 3

This service aligns with G-Cloud 15 Lot 3 by supporting:

- Independent cybersecurity assurance and readiness assessment
- Risk reduction prior to digital delivery or cloud adoption
- Governance and capability assessment for cyber risk management
- Decision support without assuming operational responsibility

It provides advisory and assurance capability to strengthen organisational cyber resilience..

8. Exit and transition

The service concludes with documented security assessments, assurance findings, and recommendations relating to the Buyer's cloud services and operating environment. Outputs are provided in formats suitable for handover to the Buyer's internal teams or to alternative suppliers.

The service supports secure transition to and operation of cloud services while maintaining supplier independence and avoiding lock-in. Outputs may be used to inform future cloud security, assurance, or delivery services procured under the appropriate G-Cloud 15 Lots or through other appropriate procurement routes.

Information assurance

Morson Praxis's information assurance capabilities support both our internal requirements for appropriate security controls and those of our Buyers. Our diverse portfolio of projects and customers means that we have extensive experience in working with information and systems at all impact levels (IL 0 to IL 6+). We are a Cyber Essentials Plus certified organisation.

Data restoration/ Service migration

We assist Buyers in the migration of data from legacy solutions to new cloud solutions.

On-boarding and off-boarding processes

Morson Praxis agrees specific on/ off-boarding processes for all work packages. Agreed processes are always tailored to the individual requirements of the engagement in question. Requirements are clearly defined and agreed with the relevant Buyer stakeholders to ensure the

effective transition of individuals or teams alongside the management of data, assets, corporate memory and operational integrity.

Combination pricing

Morson Praxis can provide multiple services in scope of G-Cloud 15 Lot 3 Cloud Support Services. Our services can be bought separately or together. Combination pricing is offered accordingly.

Service management

A Service Account Manager is allocated to each Buyer's engagement. This individual is responsible for overseeing the services in scope of the engagement, closely monitoring its progress and managing all risks/ issues to ensure that activities are delivered in accordance with the agreed assignment scope and timeframes. Through structured relationship management, our Account Manager remains in regular contact with the Buyer to ensure their ongoing satisfaction.

Service constraints

Bespoke services, such as those in scope of G-Cloud 15, Lot 3 Cloud Support Services, are not subject to specific service constraints.

Service levels

Morson Praxis recommends that we enter into performance-based Service Level Agreements with all Buyers. The implementation of bespoke service levels represents the positive obligation of both parties to deliver a mutually beneficial partnership which supports end user activities and facilitates effective measurement and monitoring of the assignment. Due to the diversity of services in scope of G-Cloud 15, Lot 3 Cloud Support Services, service levels must be closely tailored to each engagement. Agreed service levels form part of the Call-Off agreement which renders us contractually bound to deliver the agreed service levels.

Knowledge transfer

Wherever possible, Morson Praxis ensures disciplined knowledge and skills transfer from the consultant(s) to the Buyer through structured knowledge capture, documentation standards, and handover planning through all delivery phases. This ensures that learning is transferred to the Buyer as the engagement progresses – ensuring the ongoing efficiency of the assignment and full embedding of the new system/service.

Ordering and invoicing

Morson Praxis is an approved and accredited supplier to multiple CCS frameworks. We are used to working with Buyers to agree tailored ordering and invoicing processes. Payment terms are 30 days from receipt of invoice.

Termination terms

Morson Praxis's standard terms and conditions include clauses which facilitate contract termination by either the consumer or the supplier.

By the consumer	By the supplier
Termination can commence without notice in the event of a Buyer citing dissatisfaction with the service provided and the issue not being rectified within an agreed timeframe, or in the event of a material breach of contract.	In the unlikely event that Morson Praxis was to withdraw from G-Cloud 15, Lot 3 Cloud Support Services, a minimum 30 days' notice would be served. Ongoing assignment commitments would be maintained through to completion in accordance with the terms of the Framework Agreement.

Buyer responsibilities

Buyer responsibilities are closely aligned to the assignment and as such, these must be discussed and agreed with the Buyer prior to the commencement of the assignment. All responsibilities are clearly cited within the Call Off contract.

Service dependencies

Service dependencies are specific to each Call-Off. Such detail must be discussed and agreed with the Buyer prior to the commencement of the engagement.



Contact

Linton Ward – G-Cloud Account Director

Linton.ward@morson-projects.co.uk

+44 (0) 7966 158 482

morson-praxis.com/services/technology-consulting/