Crown Commercial Service
Supplier

G-Cloud 15

Defendable State Assessment Service

Atos

Table of contents

1. What is the Defendable State Assessment Service? 3

2. What does it deliver? 4

1. Digital Perimeter Assessment 4
2. People Assessment 4
3. Critical Assets Assessment 4
4. Physical Perimeter Assessment 4
5. Infrastructure Assessment 5

3. What technology does it use? 6

4. What terms apply? 10

5. Termination 11

6. How do I order? 12

7. Glossary 13

8. Why Atos 14

Crown Commercial Service Supplier

Atos

1. What is the Defendable State Assessment Service?

Atos' Defendable State Assessment is a comprehensive offensive security service designed to thoroughly evaluate a public sector organisation's cybersecurity posture against real-world threats. It is rooted in the philosophy that proactively identifying and remediating vulnerabilities from an adversarial perspective is crucial for establishing robust cyber defences.

The assessment mimics the methodologies of sophisticated attackers to provide a multi-layered, in-depth evaluation of an organisation's security posture. It consists of five modular assessments covering the:

- Digital perimeter
- People
- Critical assets
- Physical perimeter
- Infrastructure

Each assessment follows a structured approach to map the attack surface, conduct technical reviews, analyse security controls and provide detailed reporting and remediation guidance.

The Defendable State Assessment aims to help public sector organisations address common cybersecurity challenges and achieve a ‘defendable state’ - a hardened, resilient posture that effectively limits attackers' ability to penetrate and move laterally within the environment. By continuously placing ethical hackers to assess the public sector organisation's defences, Atos enables a proactive, adversarial approach to cybersecurity.

Atos’ team of expert offensive security professionals adopts an adversarial mindset, thinking like genuine threat actors to provide a realistic evaluation of an organisation's defences.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

The Defendable State Assessment service comprises five key module assessments that can be conducted individually or as part of a comprehensive programme. Each module focuses on a specific aspect of a public sector organisation's cybersecurity posture, providing in-depth evaluation and actionable insights. The five modules are:

1. Digital Perimeter Assessment

   Evaluate the security posture of the organisation's externally facing systems, including web applications, APIs, cloud-based SaaS, VPNs, network equipment, DNS records and public domains.

   Identifies vulnerabilities and prioritises remediation efforts to strengthen the frontline defence against online threats.

2. People Assessment

   Assesses the human element of cybersecurity, focusing on security awareness, policies, education and user behaviour.

   Conducts HUMINT (human intelligence) exercises, counter-phishing simulations and privileged access reviews to identify staff vulnerabilities and gaps in security training and controls.

3. Critical Assets Assessment

   Evaluate the security posture of the public sector organisation's most critical assets, such as core systems (e.g., Active Directory, ERP, e-commerce platforms), their surrounding environment, access controls and network segments.

   Identifies vulnerabilities and provides a roadmap to enhance the protection of these high-value targets against potential attacks.

4. Physical Perimeter Assessment

   Assesses the security of the public sector organisation's physical perimeter, including Wi-Fi networks, guest areas, CCTV systems, access control systems and physical barriers (e.g., fences, doors and locks).

   Identifies weaknesses that could enable cyber-attacks and provides recommendations to strengthen physical security controls.

5. Infrastructure Assessment

Evaluates the security posture of the public sector organisation's internal infrastructure, encompassing networks, servers, workstations, services, authentication processes and communication systems (e.g., VoIP).

Identifies vulnerabilities, misconfigurations, and gaps in security controls that attackers could exploit for lateral movement and privilege escalation.

Each module assessment follows the structured approach outlined in the document, including documentation review, interviews, attack surface mapping, technical review, security controls analysis and reporting. The findings from these assessments are consolidated into a comprehensive report, providing a holistic view of the organisation's cybersecurity posture and prioritised recommendations for remediation and improvement.

By conducting these five module assessments, the Defendable State Assessment service enables public sector organisations to gain deep insights into specific aspects of their cybersecurity posture, identify and prioritise risks and implement targeted improvements to establish a robust, multi-layered defence against cyber threats.

Crown Commercial Service Supplier

Atos

3. What technology does it use?

The Defendable State Assessment is delivered through a structured process that involves close collaboration between Atos' team of offensive security experts and the public sector organisation.

Process

The delivery process typically includes the following steps:

1. Scoping and Planning:

   Atos works with the client to define the assessment scope, objectives and timeline.

   The team gathers information about the client's infrastructure, assets and specific concerns to tailor the assessment plan.

2. Documentation Review and Interviews:

   Atos reviews the client's existing security policies, procedures, and documentation to understand their current security posture and practices.

   The team conducts interviews with key personnel to gather insights into the public sector organisation's security goals, challenges and priorities.

3. Assessment Execution:

   Atos' experts perform the selected module assessments (digital perimeter, people, critical assets, physical perimeter and/or infrastructure) in accordance with the agreed-upon scope.

   The team conducts hands-on technical testing, simulating real-world attack scenarios to identify vulnerabilities and gaps in the client's defences.

   Throughout the assessment, Atos maintains open communication with the client, providing regular updates and addressing any concerns or questions.

4. Analysis and Reporting:

   Atos analyses the assessment findings, prioritising vulnerabilities based on their potential impact and likelihood of exploitation.

The team prepares a comprehensive report detailing the assessment methodology, scope, key findings and prioritised recommendations for remediation and improvement.

The report is presented to the organisation during a dedicated briefing session, where Atos' experts walk through the findings, answer questions and provide additional context and guidance.

5. Remediation Support:

   Atos provides hands-on support to the public sector organisation in implementing the recommended remediation measures and improving its overall cybersecurity posture.

   The team offers guidance on best practices, assists in prioritising actions and helps the organisation develop a roadmap for continuous improvement.

6. Ongoing Collaboration:

   Atos maintains an ongoing relationship with the public sector organisation, providing support and guidance as needed to ensure the effectiveness of implemented controls and the client's continued resilience against evolving threats.

   The team offers regular reassessments to track progress, validate the effectiveness of implemented measures and identify new areas for improvement.

Throughout the delivery process, Atos emphasises clear communication, collaboration and knowledge transfer to ensure that the client gains maximum value from the Defendable State Assessment.

The team's goal is not only to identify vulnerabilities but also to empower the client with the insights and guidance needed to establish a robust, proactive cybersecurity posture that can effectively defend against real-world threats.

Benefits

The Defendable State Assessment service offers numerous benefits to organisations seeking to enhance their cybersecurity posture and establish a robust defence against real-world threats. The key benefits include:

1. Comprehensive Evaluation

   Provides a thorough, multi-layered assessment of the public sector organisation's cybersecurity posture across digital, human, physical and infrastructural dimensions.

   Offers a holistic view of the organisation's security strengths, weaknesses and areas for improvement.

2. Proactive Threat Identification

   Identifies vulnerabilities, misconfigurations and security gaps before malicious actors can exploit them.

   Enables public sector organisations to address risks and proactively minimise the attack surface.

3. Adversarial Perspective

   Assesses the public sector organisation's defences from an attacker's perspective, using real-world tactics, techniques, and procedures (TTPs).

   Provides insights into how genuine threat actors might attempt to penetrate and navigate the organisation's environment.

4. Prioritised Remediation

   Delivers a prioritised list of recommendations for remediation and improvement based on the criticality and potential impact of identified vulnerabilities.

   Helps public sector organisations efficiently allocate resources and focus on the most pressing security issues.

5. Compliance Alignment

   Aligns the assessment methodology with industry-recognised cybersecurity frameworks and standards.

   Assists public sector organisations in meeting relevant UK Government compliance requirements and demonstrating due diligence in cybersecurity.

6. Customised Approach

   Tailors the assessment scope and plan to the organisation's unique security requirements, risk profile and business objectives.

   Ensures that the delivered insights are relevant, actionable and aligned with the public sector organisation's overall cybersecurity strategy.

7. Expert Guidance and Support

   Provides access to Atos' team of experienced offensive security professionals who bring a wealth of knowledge and practical expertise.

   Offers hands-on support in implementing recommended remediation measures and improving the public sector organisation's overall cybersecurity posture.

8. Continuous Improvement

   Serves as a foundation for ongoing collaboration and continuous improvement of the organisation's cybersecurity defences.

   Provides a roadmap for maturing the public sector organisation's security posture over time, adapting to evolving threats and business requirements.

9. Increased Resilience

   Helps public sector organisations establish a defendable state, a mature and resilient cybersecurity posture that effectively limits attackers' ability to penetrate and move laterally within the environment.

   Reduces the risk of successful cyber-attacks and minimises the potential impact of security incidents across the organisation and wider UK Government services.

10. Competitive Advantage:

    Demonstrates the public sector organisation's commitment to cybersecurity and proactive risk management.

    Enhances the organisation's reputation among customers, partners and stakeholders as a security-conscious entity.

By leveraging the Defendable State Assessment service, public sector organisations can gain a deep understanding of their cybersecurity posture, prioritise risk mitigation efforts and establish a strong, adaptive defence against evolving cyber threats.

The proactive, comprehensive and expert-driven approach empowers public sector organisations to make informed security decisions, optimise resource allocation and continuously improve overall cyber resilience.

Crown Commercial Service *Supplier*

Atos

4. What terms apply?

To the fullest extent permitted under G-Cloud 15 Framework Agreement and the Call-Off Contract, Atos will provide the Services in accordance with the Atos Supplier Terms (which will include, but may not be limited to , the Supplier Acceptable Use Policy, Supplier Data Processing Agreement, Supplier Specific Shared Responsibility Model, Supplier SLAs and Supplier Licence Terms and any applicable Third-Party Terms outlined in this Service Description document and the Order Form) and this Service Description document.

For clarity:

- Atos Supplier Terms may be modified in accordance with the provisions of the Call-Off Contract, and remain effective except where expressly overridden.
- Hyperlinks included in the Atos Supplier Terms and Service Description document remain effective where they point to Atos' or the relevant Third-Party Terms or documents. Should a hyperlink cease to function, Atos will work with the client to update it through the agreed procedure.

Crown Commercial Service *Supplier*

Atos

5. Termination

Termination shall be in accordance with:

- The G-Cloud 15 Framework terms and conditions
- Any terms agreed within the Order Form of the relevant Call-Off Contract
- For this specific service, by default Atos ask for at least thirty (30) days prior written notice of termination without cause.

Atos commits to the continued provision of services for the duration of the Call-Off Contract subject to the terms and conditions of the G-Cloud 15 Framework Agreement, the Call-Off Contract, the Atos Supplier Terms and the applicable Third Party Agreements (as defined in the Atos Supplier Terms and indicated in the Order Form) related thereto.

Crown Commercial Service *Supplier*

Atos

6. How do I order?

Please contact our team at: gcloud@atos.net

- We will prepare a quotation for your review, including any applicable volume discounts.
- Once the quotation is agreed, we will issue the necessary documentation (as required by the G-Cloud Framework) and request a purchase order from you.
- Upon receipt of your purchase order, we will configure the services in line with the agreed requirements. Where applicable, you will also receive access to our self-service portal to begin provisioning services.
- If you are a new customer, you may need to complete additional 'new supplier' forms.
- Invoices will be issued to you and to Crown Commercial Service (CCS), quoting the purchase order number, for the services procured.
- We will also submit the required monthly management information reports to Government Procurement.

Crown Commercial Service *Supplier*

Atos

7. Glossary

Term	Definition
CAF	Cybersecurity Assessment Framework
GDPR	General Data Protection Regulation
M&A	Mergers and Acquisitions
MCSS	Minimum Cyber Security Standard (MCSS)
NCSC	National Cyber Security Centre
PCI-DSS	Payment Card Industry Data Security Standard
ROI	Return on Investment

Crown Commercial Service *Supplier*

Atos

8. Why Atos

Atos has been a trusted partner on every G-Cloud iteration since the framework began, helping public sector organisations modernise with confidence. We combine global expertise with deep UK experience, delivering secure, scalable cloud solutions that meet the highest government standards.

As Europe's leading provider of cloud and cybersecurity services, Atos offers end-to-end capabilities - from migration and hosting to SaaS and consultancy - supported by UK delivery centres and strategic partnerships with hyperscalers.

Our focus on innovation, sustainability, and social value ensures that customers not only achieve operational excellence but also contribute to a greener, fairer future. With Atos, you gain a proven partner committed to driving efficiency, resilience, and transformation across public service.

About Atos

Atos Group is a global leader in digital transformation with c. 67,000 employees and annual revenue of c. €10 billion, operating in 61 countries under two brands — Atos for services and Eviden for products. European number one in cybersecurity, cloud and high-performance computing, Atos Group is committed to a secure and decarbonized future and provides tailored AI-powered, end-to-end solutions for all industries. Atos Group is the brand under which Atos SE (Societas Europaea) operates. Atos SE is listed on Euronext Paris.

The purpose of Atos Group is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Learn more at: atos.net

105043-RR