Crown Commercial Service
Supplier

G-Cloud 15

Offensive Security Programme Service

Atos

Table of contents

1. What is the Offensive Security Programme Service 3
2. What does it deliver? 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 Offensive Security Programme Service

The Offensive Security Programme is a comprehensive, year-long service provided by Atos to help public sector organisations proactively strengthen their cyber defences and maintain a defendable state against potential attacks.

The programme is uniquely tailored to each organisation's requirements, strategy and business objectives, ensuring that its security needs are met effectively.

The programme employs a multi-faceted approach that includes Defendable State Analyses, Penetration Tests, and Attack Emulations.

These assessments are performed by skilled ethical hackers with deep technical knowledge who can adapt to any technology on the market.

The team works to identify vulnerabilities across the organisation's entire attack surface, including:

- External perimeter
- Privilege escalation
- Web applications
- Physical site security.

The programme offers a range of benefits to the organisation, including proactive defence hardening, expert-led remediation, measurable risk reduction, customised scheduling, compliance support and ongoing optimisation.

Atos' experts who collaborate closely with public sector organisations are certified to a high level and hold and maintain key industry certifications.

Atos' Expertise

By continuously improving the organisation's security posture and addressing new threats and technologies, the Offensive Security Programme helps public sector organisations to stay ahead of potential attackers and maintain a robust cyber defence.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

The Offensive Security Programme is a comprehensive, proactive approach to cybersecurity that aims to protect public sector organisations from potential attacks by identifying and remediating vulnerabilities before they can be exploited.

Delivered by Atos, the programme is tailored to each organisation's unique requirements, strategy and business objectives, ensuring its security needs are met effectively.

The programme is delivered using an Agile methodology, with sprint-based cycles that cover the entire organisational landscape. This approach allows for periodic improvements in the public sector organisation's cyber resilience and its ability to defend against real-world attacks.

The programme also ensures that all regulatory compliance requirements for penetration and security testing are met.

The programme employs a multi-faceted approach, which includes:

1. Defendable State Analyses
2. Penetration Tests
3. Attack Emulations

Throughout the engagement, the Offensive Security Programme provides quarterly executive reports that showcase the achieved measurable security improvements. These reports detail the risk reduction outcomes across key metrics, such as reduced attack surface, strengthened threat detection, enhanced incident response, and decreased breach impact.

Crown Commercial Service Supplier

Atos

3. What technology does it use?

Delivery Methodology

The programme is delivered using an Agile methodology with sprint-based cycles, covering the entire organisational landscape. The delivery process consists of four key phases:

1. Planning:
    - Collaborating with the public sector organisation to develop an annual testing plan based on business risk assessment, compliance needs and attack surface
    - Establishing recurring test cycles, ideally quarterly, structured around the organisation's operations and cycles
    - Developing and agreeing upon rules of engagement and reporting
2. Assessment:
    - Executing planned offensive security tests using the latest ethical hacking tools and techniques
    - Taking a hacker's view to identify vulnerabilities across the environment, including external perimeter, privilege escalation, web applications and physical site security
    - Documenting all findings in actionable remediation reports
3. Optimisation:
    - Analysing results at the management level to demonstrate security improvements over time
    - Tuning the programme based on lessons learnt to increase the effectiveness of future assessments
    - Expanding the programme to cover additional attack vectors or new assets
    - Remediation:
    - Debriefing findings with the organisation's security team and discussing mitigation options
    - Supporting prioritisation based on severity and business risk
    - Verifying successful fix of issues through follow-up scanning

Reporting and Collaboration

Throughout the engagement, the Offensive Security Programme provides quarterly executive reports showcasing measurable security improvements. These reports detail the risk reduction outcomes across key metrics, such as reduced attack surface, strengthened threat detection, enhanced incident response, and decreased breach impact.

The programme is designed to be flexible and customisable, allowing public sector organisations to set assessment priorities and extract maximum value based on their unique risk landscape, resources and objectives. The collaboration between Atos' ethical hackers and the organisation's security team ensures that the most urgent gaps, opportunities, and needs are addressed effectively.

Key Benefits

The Offensive Security Programme offers a range of compelling benefits that significantly enhance a public sector organisation's cybersecurity posture and provide tangible value to the business and its government customers.

Proactive Defence Hardening:

- Continuous ethical hacking assessments identify vulnerabilities before criminals or nation-states can exploit them, enabling a proactive rather than reactive stance.
- Recurring schedules provide more frequent and timely insights compared to point-in-time audits, ensuring that the organisation stays ahead of emerging threats.
- Testing is expanded to cover new assets, users and geographies as the organisation evolves, maintaining a comprehensive defence strategy.

Expert-Led Remediation:

- Atos' experienced ethical hackers' brief findings, provide context on risks and recommend fixes tailored to the organisation's specific technology stack
- Hands-on collaboration during the remediation process strengthens the organisation's security team's skills and knowledge, enhancing their ability to handle future threats independently
- Follow-up assessments verify the successful mitigation of identified issues, ensuring that remediation efforts are effective and complete.

Measurable Risk Reduction:

- Quantitative benchmarks demonstrate improvements in the public sector organisation's security posture over time, providing clear evidence of the programme's impact.

- Trend reports visualise the reduction in critical vulnerabilities month-over-month, enabling stakeholders to track progress and make informed decisions.
- Business context helps leadership showcase the return on investment (ROI) of security efforts, justifying the allocation of resources and budget to cybersecurity initiatives.

Customised Scheduling:

- The annual assessment plan is developed in collaboration with the organisation, aligned with their operating cycles and seasonal variability, minimising disruption to critical business processes.
- Flexibility to pause testing during business-critical periods, such as year-end, ensures that the programme does not hinder the organisation's productivity or cause undue stress on resources.
- The programme optimises the balance between security rigour and minimising productivity impacts, enabling the organisation to maintain a strong defence without compromising operational efficiency.

Compliance Support:

- The frequency and coverage of testing enable consistent compliance as regulations evolve, helping the public sector organisation stay ahead of changing UK Government regulatory landscapes.
- The programme provides audit-ready evidence, such as completed scans and remediation reports, streamlining the compliance process and reducing the burden on internal teams.
- Atos' experts offer guidance on implementing controls specific to the organisation's regulatory needs, ensuring that UK Government compliance requirements are met efficiently and effectively.

Ongoing Optimisation:

- Lessons learnt from each assessment cycle are fed back into the programme, continuously improving its effectiveness over time and adapting to the organisation's changing needs.
- The programme is continuously tuned to address new attack techniques, the public sector organisation's evolving assets and potential changes resulting from Mergers and Acquisitions activities, in addition to expanding the third-party supply chain.
- This ongoing optimisation ensures the programme's continued relevance, value and ROI in the long term, making it a sustainable and cost-effective solution for the organisation's cybersecurity needs.

By delivering these benefits, the Offensive Security Programme empowers public sector organisations and, more widely, the UK Government to take a proactive, data-driven approach to cybersecurity, reducing risk, ensuring compliance, and optimising resource allocation.

The programme's comprehensive coverage, expert guidance and continuous improvement enable organisations to build and maintain a robust cyber defence that evolves with the ever-changing threat landscape.

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