Crown Commercial Service
Supplier

G-Cloud 15

Cloud Security Investment, Validation & Optimisation Service

Atos

Table of contents

Crown Commercial Service *Supplier*

Atos

1. What is the Cloud Security Investment Validation and Optimisation Service?

Atos' Cloud Security Investment and Optimisation (CSIVO) service sets itself apart by offering a comprehensive framework designed to maximise the effectiveness and efficiency of cloud security investments.

With a strong emphasis on spend validation, CSIVO delivers a multi-faceted approach to ensure that public sector organisations get the most value from their security investments while maintaining a robust security posture.

The CSIVO service offers a comprehensive approach to enhancing and optimising cloud security investments through two key offerings:

1. An Annual Assessment
2. A Managed Service.

This service is specifically designed for public sector organisations navigating the complex landscape of cloud security, where the constantly evolving threat landscape, regulatory requirements and the need for cost-effective solutions present significant challenges.

CSIVO combines advanced technology, strategic consulting, and expert management to enable a continuously optimised, and cost-effective cloud security posture.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

The service begins with a thorough assessment of an organisation's existing cloud security infrastructure, identifying potential vulnerabilities, inefficiencies and areas for improvement. This assessment considers the unique requirements of the public sector organisation, its industry and the specific cloud platforms and services in use.

CSIVO offers a comprehensive framework to maximise the effectiveness and efficiency of cloud security investments, focusing on spend validation and optimisation. Key aspects include:

- **Strategic Investment Validation**: CSIVO provides a rigorous assessment of existing cloud security tools and services, ensuring that every pound (£) spent contributes to the strengthening of the security posture. By identifying redundancies and underused resources, CSIVO ensures that investments are precisely aligned with security needs and organisational goals
- **Cost Optimisation**: through its advanced analytics and benchmarking capabilities, CSIVO identifies opportunities for cost savings without compromising on security effectiveness. This involves consolidating overlapping tools, eliminating unnecessary licences and recommending investments in solutions that offer greater value and coverage
- **Risk-aligned Investment**: by evaluating security investments in the context of the organisation's specific risk landscape, CSIVO prioritises spending on areas with the highest potential impact on risk reduction. This targeted approach ensures that resources are allocated efficiently, focusing on mitigating significant threats and vulnerabilities
- **Transparent Reporting and Analytics**: leveraging ESProfiler, CSIVO provides transparent reporting and detailed analytics on security spend effectiveness. This visibility empowers decision-makers with the insights needed to make informed choices about future investments and adjustments to their security strategy
- **Future-proofing Security Investments**: beyond immediate spend optimisation, CSIVO assists in planning future security investments that align with emerging threats and technological advancements. This forward-looking approach ensures that public sector organisations remain agile and can adapt their security measures cost-effectively.

By focusing on these spend validation elements, CSIVO delivers a unique value proposition that goes beyond traditional security services. It ensures that organisations not only safeguard their cloud environments but also achieve financial efficiency and strategic alignment in their security investments, leveraging the sophisticated capabilities of ESProfiler for real-time insights and optimisation.

CSIVO's delivery model includes:

1. **Interactive Workshops and Assessments** The process begins with interactive workshops and assessments, where CSIVO's experts engage with stakeholders to understand their unique security challenges and business objectives. Through these workshops, CSIVO tailors its approach to align with the organisation's specific needs and risk tolerance.
2. Following the workshops, CSIVO conducts comprehensive assessments using ESProfiler to analyse the organisation's security posture, identify inefficiencies and highlight optimisation opportunities.
3. These assessments provide a detailed picture of the public sector organisation's current security state, enabling CSIVO to develop targeted recommendations for improvement.
4. **Detailed Reporting and Strategic Recommendations** We provide detailed reports that offer evidence-based insights into the efficiency and effectiveness of the deployed security technologies. These reports not only highlight cost-saving opportunities but also offer actionable remediation steps to address identified gaps and vulnerabilities.
5. **Remediation Workshops and Managed Service Support** To support the implementation of optimisation strategies, CSIVO offers remediation workshops and a managed service for ongoing security management.
6. The remediation workshops provide guidance and support for implementing the recommended changes, ensuring a smooth transition to an optimised security posture.
7. The managed service component offers continuous monitoring, maintenance and improvement of the organisation's cloud security infrastructure, ensuring that the benefits of CSIVO's framework are sustained over time.
8. By combining strategic validation, cost optimisation, risk alignment, transparency and future-proofing, CSIVO empowers organisations to maximise the value of their cloud security investments while maintaining a robust security posture.

Crown Commercial Service Supplier

Atos

3. What technology does it use?

CSIVO leverages ESProfiler, a state-of-the-art platform that revolutionises the validation and optimisation of cloud security investments. This powerful AI-enhanced tool is designed to support organisations with hybrid, full-cloud, or full-on-prem environments, providing a comprehensive solution for continuously managing and optimising security investments.

ESProfiler's advanced analytical engine combines with AI-driven intelligence, real-time threat monitoring, and continuous tracking of feature utilisation. This equips organisations with the tools needed to refine their security strategy, ensure compliance and achieve measurable cost savings while maximising return on security investments.

Key features of ESProfiler:

AI-Powered Analytical Engine with Autonomous Agents

At the core of ESProfiler is its analytical engine, now enhanced with a team of AI agents built to help security leaders automate decision-making. This engine processes vast amounts of data to identify security investment optimisations, track feature utilisation over time, and provide actionable insights. Through its partnership with Google for Startups Growth Academy, ESProfiler integrates advanced AI capabilities for proactive threat detection, automated response, and smarter risk management—all while maintaining data sovereignty and compliance requirements critical to public sector organisations.

The Capability Exchange

This industry-first infrastructure continuously tracks the evolution and utilisation of security product features throughout the contract lifecycle. Currently onboarding over 100 vendors simultaneously, the Capability Exchange enables organisations to engage vendors centrally, request information, and identify new market solutions from one platform. It provides a standardised capability model that maps security features at a granular level to frameworks, including MITRE ATT&CK, ICS, Mobile, ATLAS for AI, and NIST, allowing organisations to understand exactly what their current tools can detect and defend against.

Advanced Threat Intelligence Integration with Dynamic Prioritisation

ESProfiler's "Sightings" feature revolutionises threat intelligence by dynamically tracking observations of threat activity across over 300 feeds, government CERTs, and open-source intelligence. This real-time strategic intelligence pinpoints critical security gaps based on your organisation's specific threat profile, ensuring that security investments remain aligned with evolving attack trends. The platform transforms traditional threat feeds into strategic insights, enabling executives to make threat-informed decisions about where to allocate resources for maximum impact.

Unified Security Investment Dashboard

This comprehensive dashboard provides executives and IT teams with a real-time, unified view of security investments across all business units—not just the security budget, highlighting areas of overspend, underutilisation and opportunities for optimisation. By presenting this information in an easily digestible format, the dashboard enables decision-makers to quickly identify areas where budget reallocation can improve security outcomes and reduce costs.

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.

7. Glossary

Term	Definition
AI	Artificial Intelligence
CERT	Computer Emergency Response Team
CSIVO	Cloud Security Investment and Optimisation
SaaS	Software as a Service
SLA	Service Level Agreement

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