

**G-Cloud 15**

# **Cloud Security Configuration Assessment Service**



**Atos**

# Table of contents

|                                                                     |    |
|---------------------------------------------------------------------|----|
| 1. What is the Cloud Security Configuration Assessment Service..... | 3  |
| 2. What does it deliver? .....                                      | 4  |
| 3. What technology does it use? .....                               | 6  |
| 4. What terms apply? .....                                          | 9  |
| 5. Termination.....                                                 | 10 |
| 6. How do I order? .....                                            | 11 |
| 7. Glossary.....                                                    | 12 |
| 8. Why Atos.....                                                    | 13 |



# 1. What is the Cloud Security Configuration Assessment Service

Atos' Cloud Security Configuration Assessment advisory services provide a comprehensive evaluation of public sector organisations' cloud infrastructures, identifying vulnerabilities, configuration weaknesses and potential threats.

With a focus on Microsoft Azure, AWS and Google GCP environments, the service offers insights into current security postures and opportunities for improvement. Leveraging native cloud security services such as Sentinel, Defender, GuardDuty, Security Hub, Shield Advanced, and KMS encryption, Atos enables better adoption of cloud security best practices.

Certified teams deliver guidance on configuration, regulatory compliance, and risk mitigation strategies, empowering organisations to enhance their security posture, optimise subscription returns, and ensure data privacy in multi- and hybrid-cloud and SaaS environments.

Overall, the Cloud Security Configuration Assessment service exemplifies Atos's commitment to helping public sector organisations maximise the value of their cloud investments while ensuring the highest standards of security and compliance. By combining deep technical expertise, a best-practice-driven approach and a flexible delivery model, Atos enables public sector agencies to secure their organisation in the cloud with confidence.



## 2. What does it deliver?

The Cloud Security Configuration Assessment service offered by Atos is designed to help organisations address common challenges and concerns regarding effectively securing their workloads on Microsoft Azure, AWS and Google GCP.

These challenges often stem from a lack of skills, confidence and experience in leveraging cloud-native security controls, which can prevent public sector organisations from fully realising the security benefits of their Microsoft Azure, AWS, and Google GCP investments.

Specific organisation challenges that the service aims to address include:

- Fear of losing control and visibility over data in the cloud, especially in complex multi-cloud, hybrid-cloud and SaaS environments
- Concerns about data privacy and the risk of unintended disclosure of sensitive information
- Lack of in-house cloud security expertise and limited awareness of the security features and best practices in Microsoft Azure, AWS and Google GCP

To help public sector organisations overcome these challenges and achieve better security outcomes on Azure, AWS and GCP, the Cloud Security Configuration Assessment service delivers:

- A comprehensive assessment of the organisation's current cloud platform security posture, focusing on their adoption and configuration of core security services. This provides visibility into gaps and areas for improvement
- Actionable recommendations aligned with industry standards (like CIS, NIST, ISO 27001, PCI DSS) and Cloud best practices to enhance the organisation's cloud security posture. This gives a clear roadmap to address identified gaps and optimise their use of cloud security controls
- Hands-on support to enable and configure the in-scope cloud security services, if not already in use. This helps organisations quickly start leveraging these powerful security capabilities in their environment
- In-depth workshops and knowledge transfer sessions to improve public sector organisations' teams and give them the skills and confidence to effectively use cloud security services and implement best practices going forward.

By delivering these outcomes, the service empowers public sector organisations to strengthen their cloud security posture, gain greater visibility and control over their data in the cloud and ultimately better secure their business on cloud. Organisations can expect

a tailored engagement that fits their specific needs and environment, delivered by a team with deep expertise in cloud security best practices and a strong track record of customer success.

### 3. What is the approach?

The Cloud Security Configuration Assessment service is part of Atos's broader portfolio of cloud security offerings, which are designed to help public sector organisations secure their cloud adoption journey at every stage. This particular service is targeted at public sector organisations that have already invested in Microsoft Azure, AWS, and Google GCP and want to ensure they are effectively leveraging the native security capabilities to secure their workloads and data.

The service is delivered by Atos's team of experienced cloud security professionals who bring a wealth of expertise and practical knowledge to every engagement. Key strengths of the delivery team include:

- 50+ dedicated cloud security experts
- Experience from 50+ successful cloud security projects
- 100+ industry-recognised cloud security certifications (AWS, Azure and GCP)
- Proven delivery methodology and specialised tools
- Strong partnerships with major cloud providers and security vendors

Atos's approach to delivering the Cloud Security Configuration Assessment service is grounded in industry best practices and standards, such as:

- Cloud Security Alliance (CSA) guidelines
- Centre for Internet Security (CIS) benchmarks
- NIST SP 800-53 and 800-210 standards
- ISO 27001, 27017 and 27018 standards
- Payment Card Industry Data Security Standard (PCI DSS)
- General Data Protection Regulation (GDPR)
- FedRAMP requirements
- Well-Architected Framework and other cloud provider best practices

By aligning with these standards and frameworks, Atos ensures that the recommendations and action plans delivered through the service are comprehensive, relevant and effective in improving the organisation's cloud security posture.

The Cloud Security Configuration Assessment service is delivered through a structured engagement model that combines remote and on-site activities, tailored to the organisation's specific needs and environment. The key phases and activities of the service delivery include:

### 1. Pre-Qualification and Scoping (one week)

Pre-qualification call with Atos to assess the public sector organisations' needs and suitability for the service.

Initial introductory call with the organisation to provide an overview of the assessment, walk through the discovery questionnaire and agree on project timelines and logistics.

### 2. Mobilisation (one week)

Finalising the Statement of Work (SoW) based on the organisation's inputs and requirements.

Enablement call to confirm the start date, review any additional inputs and enable the required security services on the organisation's side.

### 3. Pre-workshop Enablement Session (if required)

Remote session to guide the organisation through enabling and configuring the in-scope cloud security services, allowing them to start gathering data for analysis in the main workshops.

### 4. Workshops (two days)

On-site or remote interactive workshops led by Atos security experts, covering the agreed scope of cloud security services.

Workshops include a mix of presentations, hands-on labs and discussions to assess the organisation's current use of these services, identify gaps against best practices and provide recommendations for improvement.

### 5. Reporting and Readout (one week)

Atos consultants prepare a summary report of the findings, recommendations and action plan from the assessment.

Readout session with the organisation to walk through the key insights and next steps from the report.

## 6. Project Closure

Atos submits a project closure report to capture organisation feedback, obtain sign-off and agree on any follow-up actions.

Throughout the delivery lifecycle, Atos maintains a strong focus on knowledge transfer and uplifting public sector organisation capabilities. The workshops and interactive sessions are designed not just to identify gaps and provide recommendations, but also to give organisational teams hands-on exposure to Azure, AWS and GCP security best practices and to empower them with the skills and confidence to manage cloud security effectively.

Post-delivery, Atos offers ongoing support to help public sector organisations execute the recommendations and action plans. This can include further advisory, implementation or managed security services, depending on the organisation's needs and in-house capabilities.



## 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.



## 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.



## 6. How do I order?

Please contact our team at: [gcloud@atos.net](mailto: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 the Government Procurement.



# 7. Glossary

| Term    | Definition                                   |
|---------|----------------------------------------------|
| AWS     | Amazon Web Services                          |
| CIS     | Centre for Internet Security                 |
| GCP     | Google Cloud Platform                        |
| KMS     | Key Management Services                      |
| NCSC    | National Cyber Security Centre               |
| PCI DSS | Payment Card Industry Data Security Standard |
| SaaS    | Software as a Service                        |
| WAF     | Web Application Firewall                     |



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](https://atos.net)