Crown Commercial Service
Supplier

G-Cloud 15

Pentest Centre of Excellence Service

Atos

Table of contents

Crown Commercial Service *Supplier*

Atos

1. What is the Pentest Centre of Excellence Service

Atos' Pentest Centre of Excellence is a comprehensive, end-to-end penetration testing service. It proactively identifies vulnerabilities and assesses the exploitability of an organisation's entire IT landscape, covering a wide range of areas such as information security, network security, application security, OS security, cloud security, OT security, physical security and social engineering.

The service is designed to be highly customisable, with testing scenarios tailored to each public sector organisation's specific industry, technology stack and compliance requirements. The Pentest Centre of Excellence team conducts thorough assessments and provides detailed reports of all discovered vulnerabilities, along with a risk-based analysis of the results.

Atos' experts collaborate closely with the organisation to develop manageable remediation tasks and provide actionable recommendations to enhance the public sector organisation's security posture. The goal is to identify and address existing vulnerabilities and, strategically, fortify the organisation's defences against future threats.

By leveraging the Pentest Centre of Excellence service, organisations can benefit from:

1. Discovering exploitable vulnerabilities
2. Detecting shadow IT
3. Supporting risk management
4. Obtaining a detailed security overview
5. Planning security improvements
6. Receiving expert recommendations on next steps

Atos' experts, who collaborate closely with organisations, are highly certified and hold and maintain key industry certifications.

Atos' Expertise

Overall, the Pentest Centre of Excellence service aims to empower public sector organisations with the knowledge and guidance necessary to minimise attack surfaces, strengthen defences and maintain a robust security posture in the face of ever-evolving digital threats.

Crown Commercial Service Supplier

Atos

2. What does it deliver?

The Pentest Centre of Excellence service, provided by Atos, is a comprehensive penetration testing solution designed to help public sector organisations proactively identify and address vulnerabilities across their entire IT landscape. The service aims to deliver a deep understanding of an organisation's exploitability status and provide actionable recommendations to strengthen its security posture.

Key deliverables of the Pentest Centre of Excellence service include:

1. In-depth penetration testing: The service conducts thorough assessments across various domains, including information security, network security, application security, OS security, cloud security, OT security, physical security and social engineering. This holistic approach ensures that vulnerabilities are identified and addressed across all layers of a public sector organisation's IT infrastructure.
2. Customised testing scenarios: The Pentest Centre of Excellence team tailors their testing approach to align with the public sector organisation's specific government, industry, technology stack and compliance requirements. This customisation ensures the service addresses the unique challenges and risks each organisation faces.
3. Detailed reporting: The service provides a comprehensive report that includes a complete inventory of identified vulnerabilities, a multi-layered analysis of the public sector organisation's security posture and a risk-based assessment of the findings. This report serves as a foundation for developing a strategic plan to enhance the organisation's security.
4. Actionable recommendations: Atos' experts provide clear guidance on remediation steps and security enhancements. They offer suggestions for fixing identified issues, improving existing protections and strengthening defences against future threats. These recommendations are customised to the public sector organisation's specific environment. They include clear instructions for implementing necessary safeguards.
5. Collaborative approach: The Pentest Centre of Excellence team works closely with the public sector organisation throughout the engagement, fostering a partnership that ensures the organisation's security needs are met. This collaboration extends to developing manageable remediation tasks and providing ongoing support to execute the recommended security roadmap.

Overall, the Pentest Centre of Excellence service delivers a proactive, customised and thorough approach to penetration testing, enabling public sector organisations to strengthen their defences, minimise risk and maintain a robust security posture in the face of constantly evolving cyber threats.

Crown Commercial Service Supplier

Atos

3. What technology does it use?

The Pentest Centre of Excellence services offered by Atos are delivered through a comprehensive, multi-stage process that encompasses the entire scope of a public sector organisation's IT landscape. The delivery process is designed to be thorough, customisable and collaborative, ensuring that each client organisation's specific security needs are met effectively.

The delivery process can be summarised as follows:

Scoping and customisation: The Pentest Centre of Excellence team works with the public sector organisation to understand their specific needs, government, industry, technology stack and compliance requirements. Based on this information, they develop a customised testing plan that aligns with the organisation's unique challenges and risks.

Penetration testing: The team conducts in-depth penetration testing across multiple domains, including:

1. **Information security:** digital footprint and open-source intelligence (OSINT) assessments
2. **Network security:** external, internal and wireless security assessments
3. **Application security:** testing of web, mobile, software and firmware applications
4. **OS security:** assessments of Windows, Linux, images and thin clients
5. **Cloud security:** testing of Azure, AWS, Google Cloud and multi-cloud environments
6. **OT security:** non-intrusive security assessments of industrial control system environments
7. **Physical security:** facility access control and bug sweep assessments
8. **Social engineering:** simulated phishing, spear phishing and whaling attacks

Analysis and reporting: The Pentest Centre of Excellence team analyses the penetration test results and consolidates the findings into a comprehensive report. This report includes a detailed inventory of identified vulnerabilities, a risk-based assessment of the findings and a multi-layered analysis of the public sector organisation's security posture.

Recommendations and remediation guidance: Atos' experts provide actionable recommendations and detailed remediation guidance based on the findings of the penetration tests. They offer suggestions for fixing identified issues, improving existing protections and strengthening defences against future threats. These recommendations are customised to the public sector organisation's specific environment and include clear instructions for implementing the necessary safeguards.

Collaboration and ongoing support: Throughout the engagement, the Pentest Centre of Excellence team maintains close partnership with the public sector organisation. They work together to develop manageable remediation tasks and to provide ongoing support for executing the recommended security roadmap. This collaborative approach ensures that the organisation's security needs are met and that they are well-equipped to maintain a strong security posture.

Available Pentest Types

The Pentest Centre of Excellence offers a wide range of penetration testing services covering various aspects of an organisation's IT infrastructure. The types of pentests offered include:

1. Information Security:
    a. Digital Footprint assessments: these assessments involve scouring surface, deep and dark web sources to uncover exposed public sector organisation data, intellectual property, configurations, diagrams, usernames, emails and sensitive documents.
    b. Open-Source Intelligence (OSINT) assessments: the team uses OSINT techniques to identify information leakage risks and evaluate external security controls to validate where public sector organisations are over-exposed online.
2. Network Security:
    a. External security assessments: these assessments target perimeter systems like firewalls, web/email gateways, endpoints and VPNs using network and application-layer attacks.
    b. Internal security assessments: the team assumes an insider threat perspective to assess the organisation's defences against lateral movement, privilege escalation, service exploitation and man-in-the-middle techniques.
    c. Wireless security assessments: the team tests corporate Wi-Fi, Bluetooth, RFID and cellular networks for unauthorised access, data interception, spoofing and jamming vulnerabilities.
3. Application Security:
    a. Web application testing: the team focuses on identifying OWASP Top 10 risks through manual and automated scanning techniques.
    b. Mobile application testing: the team assesses iOS and Android apps for vulnerabilities related to insecure communications, improper data storage, lack of tampering protections and reverse engineering risks.

c. Software application testing: the team performs code reviews, static/dynamic analysis and fuzzing to uncover memory corruption, logging, encryption, DoS and mitigation bypass risks.
d. Firmware testing: the team evaluates protocols, firmware extraction, binary reversing and hardware interfaces to identify remote exploitation and authentication bypass vulnerabilities.

4. OS Security:
   a. Windows security assessments: the team focuses on identifying privilege escalation, unquoted service paths, driver and DLL sideloading, PowerShell abuse and Kerberos exploitation risks.
   b. Linux security assessments: the team checks for privilege escalation, kernel bypasses, flawed system calls, SUID manipulation and memory corruption vulnerabilities
   c. Image testing: the team validates hardening benchmarks and security baselines using code analysis and misconfiguration checks.
   d. Thin client/kiosk testing: the team assesses protocol protections, data leakage, removable media controls and specialised endpoint hardening.
5. Cloud Security:
   a. Azure, AWS, Google Cloud and multi-cloud environment testing: the team assesses cloud-native resources, including IaaS, PaaS, serverless, containers, network security groups, storage, APIs, federation, encryption and managed services for misconfigurations, privilege escalation, data extraction and service exploitation risks.
6. OT Security:
   a. Non-intrusive security assessments of industrial control system environments: the team tests ICS network devices, SCADA systems, PLCs, proprietary protocols, hardcoded credentials, HMI manipulation, OT/IT convergence points like DMZs and remote access using ICS-tailored methodologies like CSET and CSAF.
7. Physical Security:
   a. Facility access control assessments: the team attempts unauthorised entry using social engineering, tailgating, lock picking and other techniques to evade perimeter and internal access controls.
   b. Bug sweep assessments: the team uses RF monitoring and spectrum analysis to uncover hidden surveillance devices like microphones and cameras.

8. **Social Engineering:**
    a. Phishing, spear phishing and whaling attack simulations: the team ethically simulates real-world social engineering attacks to evaluate employee susceptibility and measure vulnerability rates across roles, regions and departments.

Benefits

The Pentest Centre of Excellence provides several key benefits, helping enhance the public sector organisation's overall security posture and protect against potential cyber threats. These include:

Discovering Exploitable Vulnerabilities:

- Identifying weaknesses in systems that could allow unauthorised access
- Uncovering security gaps that attackers could exploit
- Pinpointing specific flaws that can compromise defences
- Assessing the likelihood of weaknesses being leveraged by threats.

Detecting Shadow IT:

- Uncovering rogue systems and applications outside of IT's control
- Revealing unmanaged technologies and potential threats
- Identifying unauthorised apps, services and endpoints
- Mapping out an accurate inventory of all active assets and systems.

Supporting Risk Management:

- Quantifying and prioritising risks to focus mitigation efforts
- Providing data to help determine risk tolerance and treatment
- Enabling informed decisions on security trade-offs
- Focusing resources on mitigating the most dangerous vulnerabilities
- Continuously monitoring threats and adjusting risk profiles.

Providing a Detailed Security Overview:

- Delivering a comprehensive report of the public sector organisation's overall security posture
- Offering a holistic view of existing defences and potential flaws

- Presenting a complete inventory of vulnerabilities across the entire environment
- Conducting a multi-layered analysis spanning infrastructure to endpoints
- Identifying weak links and coverage gaps.

Planning Security Improvements:

- Providing expert recommendations to enhance defences
- Identifying specific actions to increase protections
- Developing a roadmap to improve security posture systematically
- Creating a prioritised plan for phased enhancements
- Determining optimal controls and safeguards for implementation
- Establishing an ongoing strategy for maintaining defences.

Offering Recommendations on Next Steps:

- Providing expert guidance on remediation and enhancements
- Suggesting fixes for identified issues and improvements for protections
- Offering strategic advice for future strengthening of defences
- Delivering customised recommendations based on the public sector organisation's environment
- Providing clear instructions to implement specific safeguards
- Offering ongoing advisory services for executing the security roadmap.

By leveraging the Pentest Centre of Excellence services, public sector organisations can proactively identify and address vulnerabilities before malicious actors exploit them.

The detailed insights and actionable recommendations provided by the Pentest team empower public sector organisations to prioritise their security efforts, allocate resources effectively and make informed decisions to strengthen their overall security posture.

Moreover, the Pentest Centre of Excellence's comprehensive approach helps public sector organisations gain a clear understanding of their current security state, to identify areas for improvement and to develop a strategic plan to enhance their defences over time. By partnering with the Pentest Centre of Excellence team, organisations can benefit from the expertise of skilled security professionals and receive ongoing support to maintain a robust security stance in the face of ever-evolving cyber threats.

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
CSAF	Common Security Advisory Framework
CSET	Cyber Security Evaluation Tool
DLL	Dynamic Link Library
DMZ	Demilitarized Zone
IaaS	Infrastructure as a Service
ICS	Industrial Control Systems
MCSS	Minimum Cyber Security Standard (MCSS)
OSINT	Open-Source Intelligence
OWASP	Open Worldwide Application Security Project
RF	Radio Frequency
SaaS	Software as a Service
VPN	Virtual Private Network

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