Crown Commercial Service *Supplier*

G-Cloud 15

Cloud SOC Transformation Workshop Service

Atos

Table of contents

Crown Commercial Service *Supplier*

Atos

1. What is the Cloud SOC Transformation Workshop Service

The SOC Transformation Workshop Service from Atos is a dynamic workshop programme designed to deliver concrete results and accelerate maturity across public sector organisations' SOCs and their ecosystems, addressing critical questions such as: "How do we securely monitor our increasingly complex multi-cloud landscape?" and "What strategy maximises value from our security monitoring investment?"

Through focused strategic planning and expert-facilitated decision-making, this workshop empowers organisations to optimise their security operations, leveraging insights from industry experts and peer experiences to transform security operations from a cost centre into a business enabler and risk reducer.

Our interactive sessions address critical objectives, including assessing current SOC capabilities against business risk priorities, optimising operational processes to reduce alert fatigue, ensuring regulatory compliance without sacrificing security effectiveness, and enhancing incident response capabilities to reduce mean time to detect (MTTD) and mean time to respond (MTTR).

Participants gain comprehensive threat visibility across all technology environments (on-premises, cloud, remote), reduced alert overload through intelligent automation, and practical guidance on tool integration and operational efficiency. The service delivers a prioritised transformation roadmap that enables early threat detection, improves incident response, enhances regulatory compliance, and positions security as a strategic business enabler.

Crown Commercial Service *Supplier*

Atos

2. What does it deliver?

The SOC Transformation Workshop Service delivers a carefully structured, interactive workshop programme designed to help public sector organisations optimise and mature their Security Operations Centre. Delivered by subject matter experts who understand that Security Operations is central to business operations and security strategy, the service guides participants through focused planning exercises and strategic decision-making activities.

The core service components include:

Pre-workshop engagement: A week-long discovery phase where our experts collect and analyse inputs, including assessment of current challenges (resource constraints, operational inefficiencies, strategic misalignment) to ensure a tailored, organisation-specific workshop experience. Participants receive self-assessment questions to evaluate their SOC maturity across key dimensions.

Interactive workshop session: A comprehensive one-day workshop addressing the organisation's specific requirements across people, process, and technology dimensions. Participants engage in practical exercises, facilitated discussions, and strategic planning activities to identify challenges, opportunities, and transformation solutions that enhance security without creating excessive friction or requiring complete replacement of existing investments.

Post-workshop follow-up: A week-long synthesis phase processing workshop insights, culminating in a comprehensive debriefing session that delivers a clear, actionable SOC optimisation roadmap with quick wins and long-term initiatives.

Throughout the engagement, experts address critical topics, including market trends, reference architectures, operating models (including tiered analyst approaches and specialised functions), pain-point analysis across resource constraints and operational challenges, and transformation opportunities. The service includes development of a customised SOC Target Operating Model Blueprint addressing:

- **Technology Architecture:** SIEM platform optimisation, EDR integration, threat intelligence augmentation
- **People and Skills:** Tiered analyst models, training roadmaps, knowledge management
- **Process Maturity:** Incident response procedures, vulnerability management lifecycle, continuous improvement
- **Operational Model:** Service level agreements, escalation paths, collaboration frameworks.

The SOC Transformation Workshop Service combines interactive workshops, strategic planning, and ongoing support to help public sector organisations enhance their SOC capabilities, strengthen their security posture, and effectively address evolving threat landscapes, including sophisticated ransomware and supply chain compromises.

Crown Commercial Service *Supplier*

Atos

3. What technology does it use?

Workshop participants engage in interactive sessions, practical exercises, and guided discussions leveraging proven frameworks and industry best practices. The workshop addresses the full spectrum of SOC technologies and capabilities, from signature-based detection to advanced analytics, helping organisations balance investments in people, processes, and technology effectively. Content is carefully tailored to address each organisation's specific requirements, ensuring outcomes are highly relevant, actionable, and aligned with unique security needs and business objectives.

Detailed Workshop Activities:

- Introduction and Market Trends
- Engaging icebreaker activities and pre-workshop self-assessment review
- Overview of current market trends, including evolving threat landscape, ransomware-as-a-service growth, and expanding attack surfaces
- Latest Gartner research insights relevant to SOC operations and maturity
- Facilitated discussion on predictions and future directions, encouraging participant perspectives on their unique challenges

Challenges Deep-Dive

- Comprehensive review of the organisation's business strategy and existing SOC blueprint
- Analysis of specific challenge categories:
- Resource Constraints: Alert overload and fatigue, staffing shortages, and budget justification
- Operational Challenges: Fragmented tooling, visibility gaps, detection deficiencies
- Strategic Issues: Business misalignment, process immaturity, compliance vs security balance
- Architecture analysis uncovering blind spots in monitoring capabilities and data quality issues
- Discussion on why current models may be ineffective, examining technical debt and organisational misalignment

Opportunities Identification

- Building on identified challenges to uncover optimisation and transformation opportunities

- Brainstorming session identifying quick wins for immediate impact on false positive reduction
- Strategic discussion on long-term transformation, including automation and orchestration
- Prioritisation exercises ranking initiatives by business impact, implementation effort, and risk reduction
- Exploration of how to demonstrate clear ROI metrics to justify security investments

Pilot or MVP Development

- Definition of Minimum Viable Product for SOC transformation aligned with business priorities
- Planning and scoping of pilot projects addressing the highest-priority gaps
- Activity categorisation into 'Must', 'Should', and 'Could' priorities based on risk exposure
- High-level roadmap creation with phased implementation approach
- Stakeholder mapping, ensuring executive sponsorship and cross-functional alignment
- Funding and budget allocation discussions linking to measurable business outcomes

Key Takeaways and Action Planning

- Summary of primary outcomes mapped to initial self-assessment questions
- Distribution of relevant blueprints, maturity models, and implementation templates
- Best practice sharing for continuous improvement and metrics-driven enhancement
- Programme approach outline with clear success metrics and KPIs
- Scheduling of follow-up calls, capability assessments, and ongoing support sessions.

The workshop fosters a collaborative environment where participants openly share experiences, addressing questions such as "Do we have the right balance of people, process and technology?" and "Could our SOC function effectively during a major security incident?" Facilitators encourage active participation, promote knowledge exchange, and guide the generation of practical transformation solutions.

By workshop completion, participants will have gained a deep understanding of their current SOC state against industry benchmarks, identified key challenges and opportunities across all maturity dimensions, and developed a prioritised transformation

roadmap. They leave equipped with knowledge, tools, and strategies to initiate effective SOC optimisation initiatives, ultimately strengthening security posture and enhancing threat detection, response, and mitigation capabilities.

Benefits

- The SOC Transformation Workshop delivers significant value by empowering organisations to optimise and mature their SOC, transforming security operations from a cost centre into a business enabler. Key value propositions include:

Immediate Strategic Benefits

- Expert Guidance and Knowledge Transfer
- Access to seasoned subject matter experts with deep industry knowledge and practical transformation experience
- Best practice insights from successful SOC transformations across public sector organisations
- Knowledge transfer enhancing internal SOC team skills and capabilities

Objective Gap Analysis

- Independent assessment of current SOC capabilities against industry best practices
- Clear identification of critical security visibility and response gaps
- Prioritised view of vulnerabilities in existing security operations

Business-Aligned Security Vision

- Translation of technical security needs into a business risk context
- Alignment of security operations with organisational priorities
- Development of a security roadmap supporting business objectives

Operational Outcomes

- Actionable Improvement Roadmap
- Phased implementation plan with quick wins and long-term initiatives
- Prioritised recommendations based on risk exposure and implementation effort
- Clear milestones and success metrics for measuring progress

Enhanced Risk Management

- More effective threat detection and response capabilities
- Reduced dwell time for security incidents
- Improved preparedness for emerging threats and attack techniques

Resource Optimisation Guidance

- Recommendations to maximise value from existing security investments
- Identification of redundancies and inefficiencies in current operations
- Strategic guidance on staffing models and sourcing strategies.

Long-Term Strategic Value

Increased Organisational Resilience

- Better preparation for security incidents and improved recovery capability
- More adaptive security posture addressing evolving threats
- Integration of security into business continuity planning

Competitive Advantage

- Security as an enabler of digital transformation initiatives
- Enhanced customer trust through demonstrated security maturity
- Reduced security-related business disruptions

Cost Avoidance

- Reduced likelihood of significant security breaches
- Lower incident response and recovery costs
- More efficient security operations, reducing operational overhead

Compliance and Governance Advancement

- Better alignment with regulatory requirements and industry standards
- Improved security reporting and metrics for executive stakeholders
- Enhanced evidence of due diligence for audits and assessments

Access to Tools, Templates, and Best Practices

- Comprehensive toolkit including maturity models, playbooks, and implementation templates
- Accelerated implementation through proven documentation and frameworks
- Industry-standard methodologies ensuring a structured, effective optimisation approach

Ongoing Support and Guidance

- Follow-up calls and support sessions providing continued guidance throughout the transformation
- Access to expert network for queries, recommendations, and ongoing implementation support
- Regular capability assessments and purple team exercise guidance.

The workshop delivers both immediate insights and long-term strategic value, ensuring your SOC effectively protects critical business assets while demonstrating clear return on security investment.

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
EDR	Endpoint Detection & Response
IAM	Identity and Access Management
KPI	Key Performance Indicator
MTTD	Mean Time to Detect
MTTR	Mean Time to Respond
MVP	Minimal Viable Product
MXDR	Managed Extended Detection and Response
ROI	Return on Investment
SIEM	Security Information and Event Management
SOC	Security Operations Centre

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