Security Governance and Assurance

Service Definition Document

Sopra Steria

Contents

1 About Sopra Steria

1.1 Overview

About Sopra Steria

Sopra Steria, a major Tech player in Europe with 50,000 employees in nearly 30 countries, is recognised for its consulting, digital services and solutions. It helps its clients drive their digital transformation and obtain tangible and sustainable benefits. The Group provides end-to-end solutions to make large companies and organisations more competitive by combining in-depth knowledge of a wide range of business sectors and innovative technologies with a collaborative approach. Sopra Steria places people at the heart of everything it does and is committed to putting digital to work for its clients in order to build a positive future for all. In 2024, the Group generated revenues of €5.8 billion.

The world is how we shape it

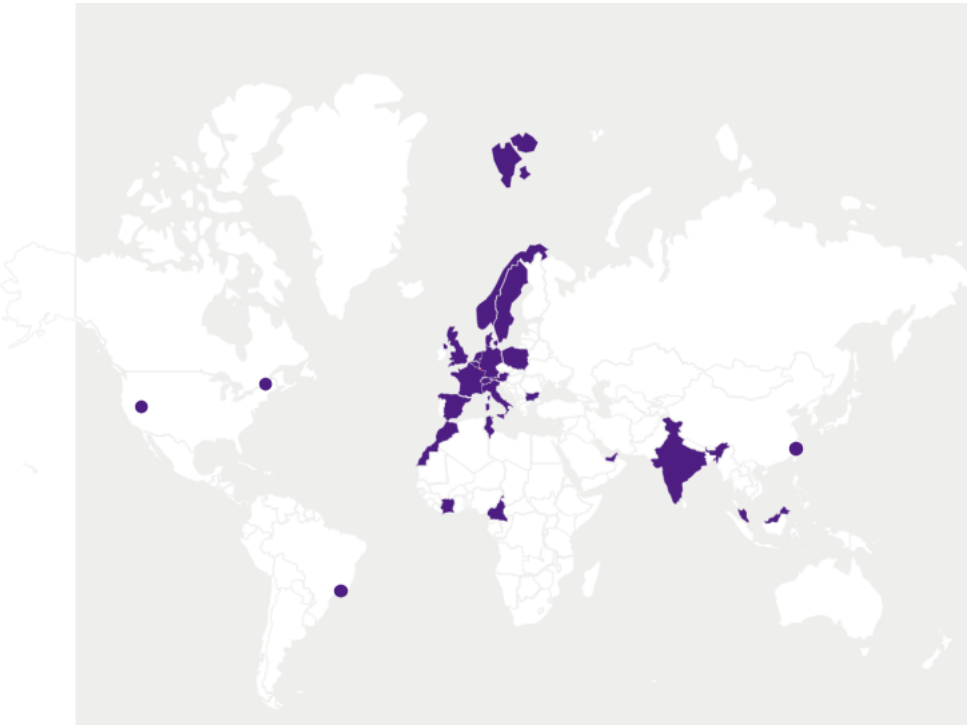
Sopra Steria (SOP) is listed on Euronext Paris (Compartment A) – ISIN: FR0000050809 For more information, visit us at www.soprasteria.com

50,000
employees

€5.8bn
2024 revenue

Top 5
European digital services companies

In nearly
30
countries



1.2 Our Cloud Capability

Sopra Steria Cloud Practice brings together leading digital, cloud and engineering expertise to accelerate transformation for our clients.

- Delivering comprehensive digital and cloud transformation, including strategic consulting, change management, large-scale migration, application modernisation, next-generation development and secure, optimised operations
- Integrating deep capability across applications, data, infrastructure, cloud platforms and security, supported by industrialised assets to enable solutions across Private, Public, Hybrid and Sovereign Cloud environments
- Using an end-to-end cloud delivery model that integrates business, engineering, security and operations, ensuring continuous innovation, strong governance, and measurable business value throughout the full cloud lifecycle.

1.3 Our Credentials

Capacity

More than 15,000 cloud experts in 30 countries (Vision, Ops, Design, Scale)

Market recognitions

- **Large account** (best category>$250m) **in the "Public Sector Industry Cloud Landscape"** (Forrester)
- **Leader "Cloud public in Europe" & " Next Gen Private & Hybrid Cloud"** (ISG)
- **Leader "Cloud Infra Brokerage"** (NelsonHall)
- **Best in Class "Azure" & "SAP" & "Service Now"** (PAC Radar)
- **Leader "Cloud Native Application" & "Application Transformation Services"** (Quadrant)
- **Major Contender "Cloud Services" & "Cloud Native Applications" & "Services on AWS Azure & CGP"** (Everest)

Key partners

NumSpot, Google Cloud, Oracle Cloud, IBM Cloud, Scaleway, vmware, aws, Microsoft Azure, Visa, OVHcloud, redhat, OUTSCALE

Main market recognitions

2nd in IT Services in France and 10th in EMEA*

Cybersecurity	Digital	AI	IT for Green	Cloud
• **Leader "Cyber resiliency services"** (NelsonHall) • **Leader "cybersecurity" in France & Germany** (ISG) • **Top 5 "cybersecurity" in France** (Markess)	• **Leader "Application Transformation Services"** (Quadrant) • **Leader "Digital Banking"** (NelsonHall) • **Leader "Digital Banking Services"** (ISG) • **Major Contender "Digital twin Services"** (Everest) • **Innovator "Digital Manufacturing"** (NelsonHall)	• **Leader AI Services & Gen AI** (PAC Innovation Radar) • **Leader AI Services** (Quadrant) • **Leader "Intelligence Process Automation"** (Quadrant) • **Major player "European Professional Services for Data-Drive"** (IDC) • **Major contenders "AI services" & "Intelligent Process Automation services"** (Everest)	• **Leader "ESG for Banking Services"** (NelsonHall) • **Best in class "consulting and digital services for sustainable development"** (PAC Innovation Radar) • **Major Contender "NetZero Consulting Services"** (Everest)	• **Large account (best category>$250m) in the "Public Sector Industry Cloud Landscape"** (Forrester) • **Leader "Cloud Infra Brokerage"** (NelsonHall) • **Best in Class "Azure" & "SAP" & "Service Now"** (PAC Radar) • **Leader "Cloud Native Application" & "Application Transformation Services"** (Quadrant) • **Leader "Cloud public in Europe" & " Next Gen Private & Hybrid Cloud"** (ISG) • **Major Contender "Cloud Services" &"Cloud Native Applications" & "Services on AWS Azure & CGP"** (Everest)

PAC, IDC, ISG, Quadrant, PEAK MATRIX, NelsonHall, FORRESTER, exægis

* Source PAC 2024

2 Service Overview

2.1 Service Description

Sopra Steria's Security Governance and Assurance team offers highly experienced consultants to support or fulfil a range of roles. This includes a CISO/Security Lead with the option of additional support from suitably qualified security specialists, including but not limited to, Security Architects and Technical Assurance consultants. Our Governance and Assurance team offer a range of capabilities operating in the governance, risk and compliance space. This can be delivered as, a standalone activity, or as part of a programme of work, the key decider being what meets the customer requirements and provides the best value and deliverables.

The Governance and Assurance team act as subject matter experts, called in as required to strengthen a customer's security posture through point in time focussed consulting engagements. If a client requires a more embedded role that takes ownership of a wider scope of security responsibilities, we can offer Operational Security Managers and/or Advisors as a service.

2.2 Features

- Structured approach to address changing business need and event response
- Governance support includes executive briefings and facilitation of working groups
- Experience to accelerate agreement of Assurance/Accreditation scope and activities
- Breadth of skills addressing a variety of risk remediation requirements
- Coordinating Assurance activities: vulnerability scanning; ITHC/Penetration tests; risks; remediation
- Support clients to develop more security aware culture and practices
- Access to additional specialist skills (SC/DV cleared) to deliver outcomes.

2.3 Benefits

- Insight to identify business risks relevant to current threat landscape
- Expertise to articulate cyber risks and obtain business sponsorship
- Insight to help prioritise risks and drive remediation effort
- Pragmatic approach based on understanding of business requirements vs identified risks
- Experience of providing advisory support across all domains of cyber security
- Access to expertise with vast experience of Public and Private sectors
- Accelerates and eases accreditation/assurance for current and changed systems
- Flexible drawdown of specialist resources
- Access to additional skills to address peaks in requirement
- Ability to produce outcomes through collaboration rather than templated solutions.

2.4 Our Approach

Sopra Steria's Governance and Assurance team consists of highly experienced security professionals covering a wide range of specialisms enabling the capture, understanding and then advising on risk. This allows us to support our customers with skilled resources aligned to specific industry sectors, business requirements and role demands.

During an engagement, the initial activity is to capture and understand the customer requirements. This enables the assignment of the correct consultant to deliver the correct outcome. Once the deliverables have been established a plan to reach them is determined and details to the customer for approval and acceptance.

The Governance and Assurance team is dedicated to tailoring the engagement to meet the customer needs, this could be for a short term or long-term period, the following are a few examples of specific capabilities that we can offer:

- Security Management; supporting or fulfilling CISO/Security Lead

- Risk Management and Assurance
- Security Maturity Assessments
- Supply Chain Security
- Information Assurance
- Data Protection
- ISMS (ISO 27001) Implementation and Audit
- Crypto Custodian Service Definition and Management
- Operational Security management in BAU environment
- Security Strategy and Direction Definition
- Security Policy Development and/or Review
- Security Process Development, Implementation and/or Review
- Incident Management Guidance
- Security Risk Assessment.

Operational Security Management is offered as a service for longer term engagements, usually delivered into a solution that is operational. Activities within the service typically include:

- Implementing strategy, policy and working practice defined within an Information Security Management System (ISMS)
- Providing regular reporting to assess the effectiveness and operation of the ISMS
- Managing and maintaining security operations in line with Security Policy, Standards and Industry Best Practice
- Understanding the customer's key objectives and to advise on areas for improvement
- Review and management of security risk and threat assessment (operational and system)
- Engagement with internal stakeholders and third party service providers on matters of information security, risk and privacy
- Managing and responding to security related incidents, developing strong internal and external relationships to promote the early identification and resolution of incidents
- Proactive management of threat detection and vulnerability management services and co-ordinating identified remediation activities
- Representing security considerations through assessment and triage of IT, process change and/or change requests
- Providing regular management reporting on the security posture and performance of key suppliers, and analysis of security related incidents
- Leading monthly client Security Working Group meetings.

The Governance and Assurance team understand the importance of meeting customer needs and expectations. Time is taken to capture and understand the requirements to then create an engagement that delivers an outcome of value that strengthens our customers' security posture.

2.5 Inputs

We would anticipate the following inputs from you as part of this service:

- Initial details of your full requirement. This will then set the approach to the next input requirements, which could include:
    - Security Framework details if proprietary
    - Security documentation.

This is a high-level list and is not exhaustive. If you don't currently have these types of input, then we would be happy discussing altering our approach to accommodate your situation.

2.6 Outputs and Deliverables

Some of the outputs and deliverables generated from the service are identified below:

- Experienced and qualified Cyber Security resources
- Created and/or improved ISMS documentation including security policies, procedures, reports etc.
- Implemented and/or improved security processes
- Strengthened security capability built on trusted relationship with stakeholders including senior Leadership Teams, business areas, IT functions, 3rd Party suppliers, audit/compliance teams and external regulatory bodies.

This is a high-level list and is not exhaustive.

2.7 Certifications and Skills

A selection of our certifications and skills related to this service is detailed below:

- CISSP - Certified Information Systems Security Professional
- CCSP - Certified Cloud Security Professional
- ISO27001 Lead Auditor
- ISO27001 Lead Implementer
- CISMP - Certificate in Information Security Management Principles
- CISM - Certified Information Security Manager
- Certified EU GDPR Practitioner
- PCI Professional (PCIP).

This is a high-level list and is not exhaustive.

2.8 Case Study

Client: Ministry of Defence

The challenge: As a part of a large Transformation Programme to redesign and relocate MoD systems and services from on-premises to a cloud hosted solution, the customer required specialist security skills and experience across a range of roles.

What we delivered: A team of Cyber Security specialists were deployed to the programme including Security Lead, Senior Information Risk Advisers (SIRAs), Security Assurance Co-ordinator (SAC), Security Architects and Security Managers.

The Security Lead was in place prior to contract start and built the security team through service transition into transformation, this ensured that a strong and trusting relationship was built with the customer. Secure processes were defined and implemented and delivery teams were provided with security guidance. Deliverables were assured as compliant with agreed policies and met customer expectations from a security perspective.

Outcome:

- Trusted and respected Security team receiving regular positive feedback from the customer
- Security Assurance documentation based on Accreditation requirements and Secure By Design principles
- Security artefacts including, but not limited to, updated policies, security awareness material, managed risk register and remediation plans
- Successful delivery of Transition and Transformation milestones approved by Customer Accreditor and Security stakeholders.

3 Pricing

Please refer to the Pricing Document for this Service.

4 Next Steps

4.1 Contact

Please contact us if you would like to know more about this service or any of our listings on G-Cloud.

Email: sector-support@soprasteria.com

As all our G-Cloud enquiries initially come into a single contact, please remember to tell us:

- Your name, your organisation name and contact details
- Which service you are enquiring about
- A summary of your requirements or problem statements that you would like support to address.

4.2 More Information

More information about our services and capabilities can be found on our website here.