Cyber Security Assessment

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

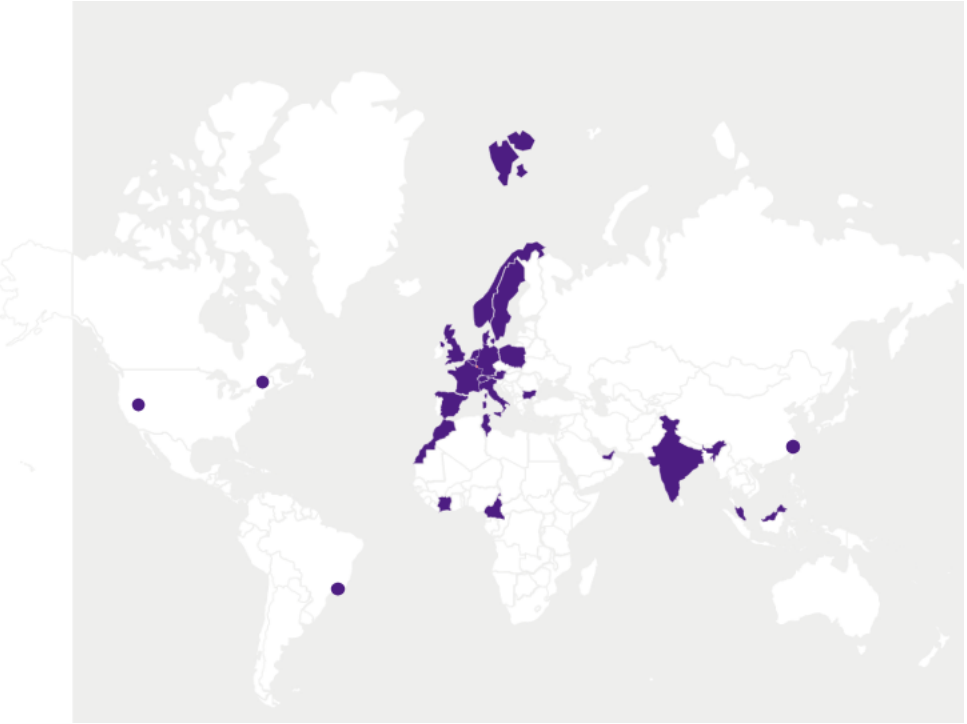
Sopra Steria (SOP) is listed on Euronext Paris (Compartment A) – ISIN: FR0000050809 For more information, visit us at www.soprasteria.com

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

Cyber Security Assessments provide an effective way to determine the security posture of an organisation and identify areas for improvement through questionnaires, interviews and workshops against industry recognised security standards including ISO 27001 and 27002, NIST Cyber Security Framework, CIS Top 20 and the Information Security Forum (ISF) Standard of Good Practice.

The aim of the service is to:

- Provide a clearer understanding of the risks and threats faced by the customer in respect of their security capability
- Identify areas for improvement, to get to a position, which delivers the appropriate capability level for their business
- Provide a prioritised action plan, targeted to achieve an informed and balanced security posture, with the required security capability and maturity.

2.2 Features

- Benchmark an organisation's information security posture against industry recognised standards
- Recommend areas for security improvement aligned to organisational objectives
- Provide a high-level prioritised action plan to realise improvements
- Engage with key stakeholders through questionnaires, interviews and workshops
- Support clients to develop more security aware culture and practices
- Opportunity to combine assessment process with penetration testing services
- SC and DV cleared staff to deliver outcomes if required.

2.3 Benefits

- Capture and understanding of security posture through detailed report
- Executive view of key findings and recommendations
- Better understanding of risks and vulnerabilities affecting information security
- Cost benefits of removing insecure or duplicated security processes and controls
- Engagement of key stakeholders to ensure awareness and buy-in
- Recommendations and prioritised roadmap for security improvement
- Solutions joining technical and business process relating to cyber security
- Ability to produce outcomes through collaboration rather than templated solutions
- Experience of providing advisory support across all domains of cyber security
- Expertise to articulate cyber risks to all levels of audience.

2.4 Our Approach

Sopra Steria's Cyber Security Assessment service is based on the use of questionnaires, interviews and workshops with relevant customer teams and third-party providers. We recommend that it is evidenced based with the relevant depth of analysis ranging from; a light touch audit with anecdotal statements backed up by visibility of supporting documentation; to a deep dive of processes and implemented controls in workshops, combined with penetration testing and vulnerability scans available from Sopra Steria as additional services.

Sopra Steria are experienced in the use of assessment tooling such as the Information Security Forum (ISF) Healthcheck tool, against the ISF Standard of Good Practice which is aligned with NIST Cybersecurity Framework (CSF), Center for Internet Security (CIS) Critical Security Controls, ISO/IEC 27002:2022, Payment Card Industry

Data Security Standard (PCI DSS) and COBIT 5 for Information Security.

The assessment can be tailored to include control questions across a range of security categories, for example the clauses listed here from ISO/IEC 27001:2022:

- Organisational Controls
- People Controls
- Physical Controls
- Technological Controls.

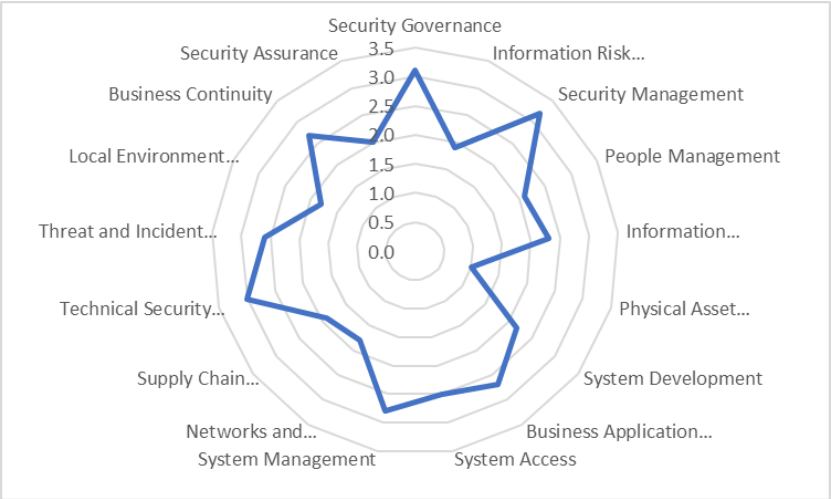
We deliver this service through engagement with Senior management, Business Stakeholders, Technical and Service owners with a view to supporting the following outcomes:

- Determine the maturity of security programmes, processes and capabilities in place
- Identify areas of strength and opportunities for improvement within these areas
- Make recommendations to align security posture against industry best practice and business objectives; and
- Initiate improvement based upon threat intelligence, current capabilities and engagement of key stakeholders.

Each assessment would typically include the following activities:

- **Scoping** – Agree scope of each assessment including IT systems, services, locations, business units, standards to measure against and security controls to assess
- **Planning** – Identification of available documentation and customer stakeholders relevant to the security control being assessed. Confirmation of attendee availability for workshops
- **Documentation review** – Policies and procedures relating to the assessment subject e.g. Asset Management will be reviewed prior to workshops. Documentation will need to be made available to Sopra Steria in advance
- **Workshops** – Meeting (face to face or online) with stakeholders to discuss the assessment subject through process walkthrough and follow-up questioning
- **Evidence Gathering/Observation** – Onsite and/or offsite review of evidence to support information determined during workshops and provide assurance that controls have been appropriately implemented
- **Analysis and reporting** – Offsite analysis of assessment findings and creation of report including recommendations for improvement
- **Closing meeting** – Meeting(s) to discuss findings, recommendations and next steps.

Report results can be presented in a variety of forms including graphical charts such as this example showing scores against ISG Standard of Good Practice categories.



A Security Lead will be allocated for each engagement to provide a point of contact and escalation path for any questions or issues that arise during the service. They will be responsible for overseeing the entire engagement and will be responsible for delivering final report, executive presentations, and high-level solution recommendations.

2.5 Inputs

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

- Access to relevant stakeholders including attendance of scheduled interviews and workshops
- Access to documentation relevant to the scope of assessment
- Facilities including meeting rooms and internet access for any part of assessment to be performed on customer sites.

This is a high-level list and is not exhaustive. If you cannot provide all of these inputs, then we can discuss 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:

- Security Assessment Report containing:
    - Assessment scoring for results mapped to customer's chosen standard(s)
    - Overview of the customer's Information Security posture
    - Identified areas for improvement
    - Recommendations and prioritised roadmap for security improvement.
- Executive presentation containing key findings and prioritised roadmap.

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

2.7 Certifications and Skills

Some of our certifications and skills related to this service are identified 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: Cabinet Office Joint Venture

The challenge: The customer required an analysis of implemented security controls (technology and process based) to determine existing capability to withstand a cyber-attack such as ransomware.

What we delivered: Sopra Steria assessed the customer's corporate security controls through discovery workshops and analysis of supporting evidence. The results of the workshop assessment were combined with technical security assessments incorporating technical audit, Open Source Intelligence (OSINT) gathering and internal network penetration testing.

Our Security Governance and Assurance specialists analysed the information received from workshops and evidence received. The output of the technical assessments and the ISF Security Healthcheck tool was utilised to generate a maturity score for each security category and an overall score for the organisation.

Outcome:

- Findings determined through the assessment that were considered high risk were shared with the customer's security team as soon as they were identified. A significant vulnerability was identified during the technical assessment. This early notice allowed mitigation plans to be agreed and implemented in advance of publication of the final report to reduce potential impact.
- The approach of encouraging discussion of security controls rather than a series of questions and answers during workshops allowed development of trust and collaboration between Sopra Steria and the customer. Our Security Governance and Assurance Specialists were able to share examples of industry good practice and guidance based on their experience during discussions. This led to openness and a feeling of inclusion for workshop attendees.
- The Assessment report was presented to senior management. This had the dual effect of identifying areas for improvement while highlighting the positive findings to show the value of implemented controls and the work of the customer's security function.

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.