Security Architecture

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

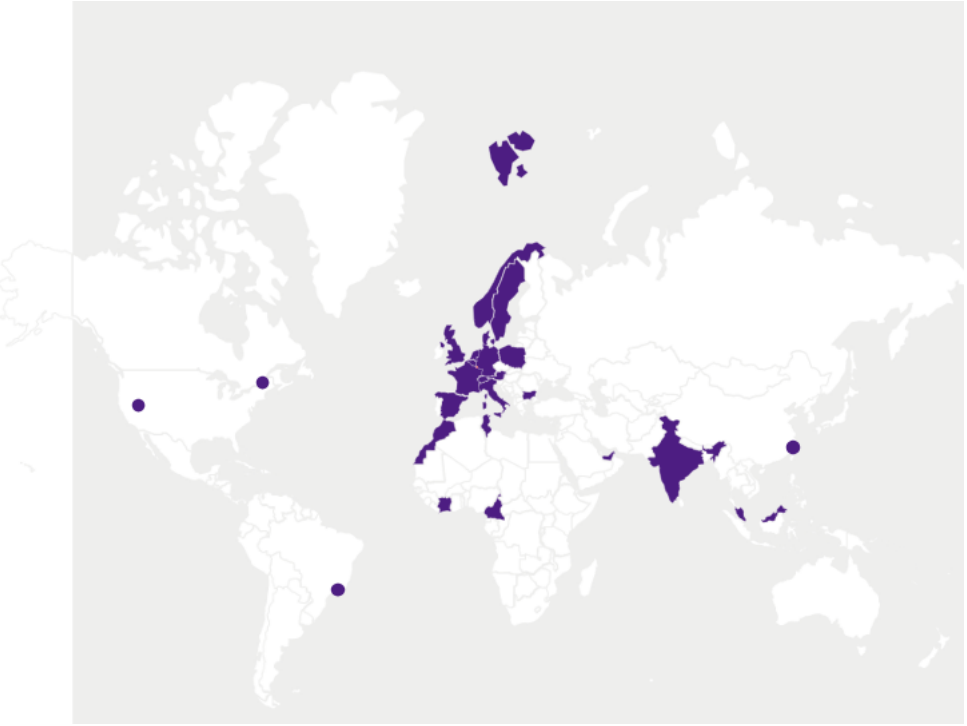
Sopra Steria (SOP) is listed on Euronext Paris (Compartment A) – ISIN: FR0000050809 For more information, visit us at www.soprasteria.com

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, Everest Group PEAK MATRIX, NelsonHall, FORRESTER, exægis markess

*** Source PAC 2024**

2 Service Overview

2.1 Service Description

With the proliferation of cloud adoption and organisation's embracing various cloud deployment models, such as hybrid and multi-cloud, and cloud service models such as Infrastructure-as-a-Service (IaaS), and Software-as-a-Service (SaaS), cloud security challenges are increasing, demanding robust, flexible and scalable security architectures to protect against the evolving cloud threat landscape.

Sopra Steria's experienced, cloud certified Security Architects, specialise in understanding business requirements and objectives. Specifically regarding our clients' use of cloud services, identifying key threats, documenting risks, and ensuring they are mitigated with appropriate technical security controls. We support many Central and Local Government clients to embed security best practices and secure by design (SbD) principles into their solutions from the outset, to ensure that security is baked in, rather than bolted on. We take a risk-based approach, based on industry-standard security architecture frameworks, and will design flexible controls to address the current and future cyber security threat landscape.

2.2 Features

- A pragmatic and structured approach to embedding cloud security architecture best practices and secure by design principles
- Ensure security controls are identified early in the design phase, rather than "bolted on"
- Design of security controls using a Risk Based Approach based on the threat context
- Development of Security Architecture related documentation, such High Level Design, Roadmaps, and Gap Analysis
- Experience of legacy architectures as well as modern, cloud-based architectures across the major CSPs, including AWS, Azure and OCI
- A well-defined Threat and Risk Assessment methodology
- Knowledge and experience of supporting clients using either the UK Government or MOD versions of Secure by Design, and
- Cloud certified Security Architects benefitting from various clearances, such as SC, DV, and NPPV.

2.3 Benefits

- Alignment to tried and tested security architecture frameworks (e.g. TOGAF and SABSA), and risk assessment methodologies, such as the ISF's IRAM
- Compliance with industry cloud security standards, such as NCSC and NIST
- Guidance from enterprise cloud providers such as AWS, Azure, Oracle and generic Cloud Security principles and best practices
- Security architecture gap analysis and security control roadmaps that align organisational plans with regulatory and contractual requirements
- Design and document the detailed implementation of cloud security controls, mitigating identified threats and risks, and reducing the organisational attack surface
- Embedding secure by design principles, bringing security 'to the left' and understanding the requirements earlier in the design phase
- Support a risk-based approach to security controls, a pragmatic approach based on understanding of business requirements vs identified risks, and
- Fostering and maintaining strong stakeholder relationships and providing confidence that proposed security controls support client objectives.

2.4 Our Approach

Sopra Steria's Security Architecture Practice brings together a team of highly experienced and accredited security professionals, including cloud-certified specialists. Covering a broad spectrum of technologies and disciplines, we support clients across their diverse security requirements. Our risk-based approach ensures that business requirements and desired outcomes are carefully balanced with the design and recommendation of appropriate security controls, all tailored to the specific threat landscape in which our clients operate.
Our approach is based upon expert knowledge of industry guidance such as NCSC, NIST, alignment with regulatory and organisational standards, including best practices from the Cloud Security Alliance, and benefits from the principles of SABSA and TOGAF.

We start by gaining a clear understanding of business objectives, client requirements, and the critical assets or services that need protecting. From here, we define and agree upon a tailored engagement scope, unique to each client's needs, and continue to collaborate closely with stakeholders throughout our engagement.

Our recommended approach beings with a threat modelling and risk assessment exercise, enabling us to design relevant, measured, and appropriate, security controls based on the specific threat landscape. We document our recommendations, providing detailed definitions of each control within formal security design documentation, identifying the risks the controls will mitigate. Additionally, our team support the scoping and analysis of security testing activities, such as ITHCs, to ensure they provide evidence of the effectiveness of the security controls, offering confidence to our clients.
The following are examples of specific capabilities that we can offer:

- **Security Leadership:** we lead security initiatives for major client engagements, fostering strong stakeholder relationships and aligning controls with business and contractual objectives,
- Tailored Security: we translate client requirements into custom security solutions, based on their bespoke requirements,
- **Secure Architecture Assessment:** we assess cloud architectures for risks, apply secure design principles, and recommend mitigating controls,
- **Security Documentation:** we document the detailed implementation of security controls in security designs documents and define testing requirements,
- **Threat Modelling:** we perform Threat Modelling using methodologies such as STRIDE or PASTA, map threats to the ATT&CK Mitre Framework and identify prioritised risks,
- **Secure by Design**: we support clients on their Secure by Design requirements, using Ministry of Defence or UK Government approaches, where applicable, and
- **Strategic Security Roadmaps:** we build security control roadmaps that align organisational plans with regulatory and contractual requirements.

Two of our services are outlined in more detail below.

2.4.1 Threat and Risk Assessment

Our Threat Modelling and Risk Assessment service leverages the ISF's IRAM2 methodology. This is combined with technical threat modelling, using methodologies and frameworks such as STRIDE and MITRE ATT&CK. Our Governance, Risk and Compliance specialists also perform non-technical threat analysis to ensure there are appropriate security controls to mitigate each identified risk. This structured, multiphase approach delivers a holistic view of organisational risk across both technical and non-technical domains.
Activities include:

- Solution Profiling
- Business Impact Assessment (BIA)
- Threat Assessment
- Vulnerability Assessment
- Risk Assessment
- Risk Treatment
- Technical controls assurance.

Our service is designed to generate actionable insights for our clients, and the result of these activities is a set of risks, which are reviewed and consolidated into a Risk Evaluation Dashboard. This provides clear, prioritised visibility of the organisation's security posture, guiding the design and deployment of effective controls.

2.4.2 Secure by Design (SbD)

Sopra Steria has successfully embedded Secure by Design principles into complex client environments, applying UK Government and Ministry of Defence methodologies, where appropriate, and always guided by a risk-based approach.

Our experience spans multiple sectors, supporting organisations new to continual assurance, as well as those transitioning from legacy accreditation models. Through our proven approach, we enable teams to integrate effective cybersecurity from project inception, delivering resilience and assurance throughout the entire lifecycle of digital service delivery.

Our defined process for Secure by Design is mapped to both the MoD's seven SbD Principles, or the UK Government's ten SbD Principles, ensuring alignment with recognised best practices. A sample set of activities include:

- **Requirements Gathering:** We align business, functional, and non-functional requirements to create a shared understanding within the context of risk appetite
- **Supply Chain Assurance:** We assess and validate third-party components and suppliers against industry standards, ensuring risks from external dependencies are effectively mitigated
- **Threat Assessment:** Leveraging the MITRE ATT&CK framework, we pinpoint relevant risks and map them to mitigating technical controls, guided by industry-leading NIST standards
- **Control Documentation:** We document controls and track their continued adherence to existing and newly observed threats, including testing and validation
- **Continuous Assurance:** We provide full lifecycle assurance by documenting controls and verifying their continued effectiveness through proactive monitoring, testing, and validation against new and existing threats, and
- **Feedback Loops:** We ensure seamless sharing of insights and proactive updates at every phase of the lifecycle.

Our process supports our clients in identifying, assessing, and mitigating cyber risks early and continuously. It provides structured guidance for integrating security into design decisions, documentation, and assurance activities, thereby strengthening the resilience and trustworthiness of all deliverables provided to the client.

2.5 Additional Services

Our Security Architecture Practice also supports wider Sopra Steria business activities in their client engagements, providing security expertise and guidance in the following areas:

- Secure Networks
- Cross-Domain Data Escalation
- Multi-Cloud Deployment
- Identity Management
- Secure Edge Deployment, and
- Simulation and Training.

All of these additional services are delivered in alignment with secure by design principles, providing confidence, resilience, and assurance for mission critical operations.

2.5.1 Secure Networks

Sopra Steria specialises in the design, procurement, installation, configuration, and ongoing support of secure network solutions operating across a wide range of available bearers. Over a considerable number of years, we

have delivered and managed networks on behalf of Defence and National Security customers in support of both operational activity and training environments. Our expertise spans:

- Wide Area Networks (WAN)
- Software Defined Wide Area Networks (SD WAN)
- Local Area Networks (LAN), and
- Wireless Local Area Networks (WLAN).

These capabilities are delivered across multiple security tiers, utilising both commercial and sovereign grade encryption technologies to ensure robust protection and assured performance. We also provide field deployable network solutions, integrating commodity bearers such as Starlink satellite services and home broadband to enable secure, flexible connectivity in dynamic or remote environments.

Our trusted technology partners include Cisco, Fortinet, L3Harris, PentenAmio, and many others, ensuring access to proven, industry leading solutions.

2.5.2 Cross Domain Data Escalation

Sopra Steria possesses extensive experience in the design, procurement, installation, configuration, and ongoing support of secure cross-classification data movement capabilities.
Our solutions include:

- Browse-down functionality for users operating on higher-classification networks, and
- Data and code escalation services that enable develop-low, deploy-high workflows.

These capabilities are engineered to support assured, secure, and efficient information exchange across classification boundaries.

2.5.3 Multi-Cloud Deployment

Sopra Steria delivers a range of multi-cloud deployment solutions to our clients and has extensive experience in the design, configuration, management and ongoing support of them.

We can deliver solutions across all classification levels.

2.5.4 Identity Management

Sopra Steria delivers a range of Identity Management solutions to our clients and supports them with extensive experience of:

- Public Key Infrastructure (PKI) services
- Secrets Management
- Single Sign On (SSO) technology
- Identity Federation
- Privileged Access Management (PAM), and
- Privileged Identity Management (PIM).

We can deliver solutions across all classification levels.

2.5.5 Secure Edge Deployment

Sopra Steria delivers a range of multi-sized edge compute solutions designed to operate at all security classifications including:

- Human-transportable, low-SWaP (size, weight and power) systems
- Vehicle-mounted or integrated platforms, and
- ISO-containerised deployments for larger, mission-scale requirements.

Our edge environments support IaaS, PaaS, and SaaS service models, enabling secure collaboration, data processing, and application hosting directly at the point of need.

Configurations can be tailored to provide reach-back connectivity and enhanced survivability, ensuring resilient operations across diverse scenarios and contested environments.

2.5.6 Simulation and Training

Our simulation platforms replicate real-world systems to support training, experimentation, testing, and solution development across a wide range of operational contexts.

They are architected for seamless integration with an extensive ecosystem of third-party capabilities—including live surveillance feeds, external simulators, and prototype applications—using industry-standard interfaces to ensure interoperability and flexibility.

By leveraging digital twin technologies, we provide highly realistic environments for modelling real-world scenarios, validating concepts, and rapidly prototyping innovative ideas with confidence and precision.

2.6 Inputs

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

- An understanding of your strategic goals, and specific security requirements tied to business priorities, including risk appetite
- Access to supporting documentation or artefacts, such as cloud architecture diagrams, or solution design documents
- Information regarding your regulatory requirements or applicable standards, and
- Dedicated resources assigned and available to support workshops, calls etc., to ensure timely collaboration and communication.

This list is intended to be high-level overview and is not exhaustive. Should you be unable to supply these inputs, we can explore adjustments to our approach to better accommodate your circumstances.

2.7 Outputs and Deliverables

Outputs and deliverables will be dependent on the agreed scope and the nature of the engagement; however, a sample list includes:

- A tailored threat and risk assessment document, including threat model
- A Cloud Security Architecture Design document
- A security controls gap analysis, using NIST CSF or NCSC's Cloud Security Principles, for example
- A Security Controls implementation document, and
- A Security Controls roadmap and recommendations document.

This list is intended to be a sample only and is not exhaustive.

2.8 Certifications and Skills

Some of our general and cloud specific certifications and skills related to this service are identified below:

- SABSA Chartered Security Architect
- The Open Group - TOGAF
- CISSP – Certified Information Systems Security Professional
- CCSP – Certified Cloud Security Professional
- CCSK – Certificate of Cloud Security Knowledge

- Extensive Cloud Service Provider certifications (AWS, Azure, Oracle).

This list provides a high-level overview of the certifications achieved by the team and is not exhaustive.

2.9 Case Studies

Client 1: BlueJay Secure Collaboration (BSC)

The challenge: In an age where the threat from hostile actors has never been greater, keeping data safe is non-negotiable. The challenge was to enable secure collaboration and communication, across the globe, so classified information could be shared between government, industry and partners internationally with integrity and assurance.

What we delivered: Bluejay is a secure collaborative working environment at SECRET that addresses this challenge for our clients.

Our team applied the Ministry of Defence's Secure by Design framework, underpinned by NCSC security principles and MoD Joint Service Publications, to embed security throughout the system lifecycle. Working in partnership with the client and independent assessors, we documented and evidenced the security controls to provide assurance and transparency.

Key activities included:

- Documenting assurance against NIST CSF requirements, to align with MoD's SbD approach
- Clearly defining a RACI model
- Continuous risk assessments throughout the project lifecycle, based on NIST SP 800-30 and SP 800-37
- Designing tailored security controls, based on NIST SP 800-53
- Assessing and continuously monitoring the risk posture of our 3rd party suppliers, and
- Applying continuous security scanning, risk tracking, and threat update analysis to validate that controls remained effective over time.

Outcome:

BSC is the only collaborative working environment of its type to be assured by Defence Digital, Ministry of Defence, against the latest cyber security threat landscape.

Client 2: Financial Services Client

The challenge: Following an independent audit by a third-party Audit and Assurance organisation, it was identified that the client lacked a formal threat modelling capability and had no documented threat assessment process. This gap meant that critical threats to their services were not being systematically identified or prioritised.

What we delivered: We deployed a team of highly skilled specialists, including Security Architects and GRC consultants, to deliver a tailored Threat and Risk Assessment. Key activities included:

- Conducting a STRIDE assessment to establish a structured threat model
- Mapping STRIDE outputs to relevant MITRE ATT&CK tactics and techniques
- Integrating these tactics and techniques into the IRAM2 risk framework
- Producing a detailed report on the client's current security posture, highlighting outstanding risks and recommending mitigating controls.

Outcome:

The engagement delivered tangible improvements to the client's security governance and risk management processes, coupled with real world threat analysis so the client gained a clear understanding of their true security

posture. The assessment confirmed strong coverage across some areas, while also presenting a transparent view of where their residual risks were located. This enabled the client to confidently plan remediation activities based on impact and likelihood, ensuring a more proactive and strategic approach to risk management.

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.