

Service Description

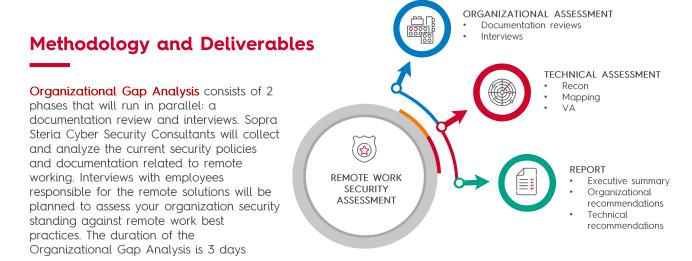
As the modern working environment changes and evolves, organizations across nearly every sector are adjusting their operating models, resulting increased remote access and work. This turn to remote work is also linked with a major rise in cyber attacks.

Sopra Steria will assess the **organizational** and **technical** aspects of your remote access and telework solutions to identify any vulnerability that may pose a significant risk for your organization.

Organizations will gain visibility about remote work infrastructure, related policies, security controls and possible weak points.

A final **report** will include a tailored, actionable recommendations that will reduce risk, and minimize the likelihood, impact, and cost of a security incident caused by misconfigured or compromised remote work solution.

The duration of the assignment is 5 working days



Technical Assessment consists of Reconnaissance, Mapping and Vulnerability Analysis of the external infrastructure related to remote access. Sopra Steria Cyber Security Consultants will perform active and passive reconnaissance, mapping and vulnerability scanning to identify the external attack surface, potential misconfiguration, exposed services and vulnerable components. The duration of the Technical Assessment is 3 days

The final **Report** includes an executive summary, the detailed results of the above assessments and actionable recommendations. The final Report will be delivered 2 days after the completion of the assessment.

