Certifications

SAS hosts solutions for privacy-conscious industries. As a result, SAS' security policies and controls are regularly audited by third parties, including customers and SAS' own auditors. This allows SAS to maintain its certifications (SOC 2, SOC 3, ISO 27001, etc.). These certifications are designed to help service organizations build trust and confidence in their service delivery processes and controls.

ISO 27001

SAS has obtained an ISO 27001 certification. The scope of the certification includes the information security management system (ISMS) based out of SAS' corporate headquarters that is limited to:

- The documented policies, processes, and controls implemented for the hosting and management of customer environments that are hosted and/or managed by SAS at SAS' corporate headquarters.
- SAS' documented policies, processes, and controls that extend globally to:
  - SAS' co-location data centers.
  - SAS' virtual private cloud at cloud service providers.
  - The remote management of the software and services of customer environments by SAS.

The statement of applicability includes control objectives from the ISO 27002:2013, ISO 27017:2015, and 27018:2019 framework.

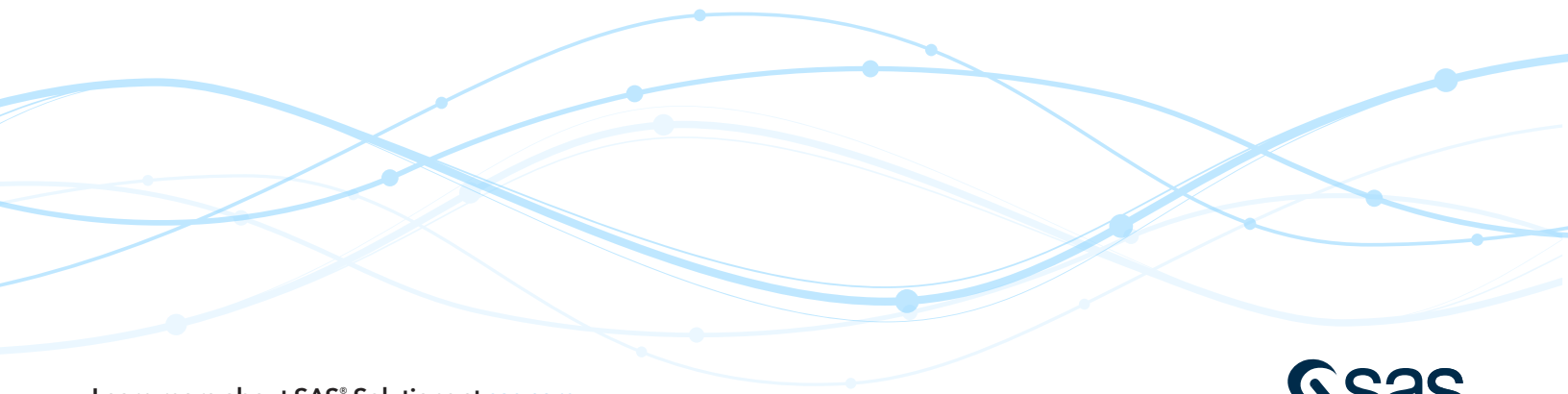
Multiple SAS country offices have also obtained ISO 27001 certifications specific to the services provided at those locations.

In addition, third-party cloud service providers and co-location data centers utilized by SAS have obtained ISO 27001 certifications specific to the infrastructure at those locations.

Service Organization Controls (SOC)

SAS engages an independent third party to perform an annual SOC 2 Type II audit certification, which includes a SOC 3 general-use report. The SAS SOC 2 Type II and SOC 3 reports pertain to the security, availability, and confidentiality trust principles and include controls related to the in-scope data centers' physical security and environmental safeguards, logical access, change management, monitoring, risk assessment and management, communication and information, systems operations, and availability over network devices as described in the report for the defined effective period. As SAS expands its services, the scope of the SOC audit will appropriately increase based on establishment, monitoring, and audit cycles.

SAS relies on third-party co-location data centers' and third-party cloud service providers' SOC 2 Type II reports to gain assurance over the applicable physical security and environmental controls related to the infrastructure, power, and data connectivity at these locations.



Learn more about SAS® Solutions at sas.com.