WHITE PAPER

APRA CPS 230

Contents

Release Information
The information in this document was current as of October 2024.

Introduction

Overview

SAS believes that businesses of the future will be hyperintelligent, artificial intelligence (AI)-driven organizations that can provide personalized, trusted customer experiences, as well as meet risk and compliance mandates.

SAS continues to deliver a trusted suite of advanced analytics and AI services. This document is part of SAS' ongoing commitment to help businesses confidently assess their risk when adopting SAS services to facilitate regulatory compliance.

This document contains:

- Help for businesses to understand SAS as a company and its typical service offerings.
- Information on APRA CPS 230 that may impact customer adoption of SAS services.
- A checklist of how SAS helps organizations to remain compliant with those regulations.

SAS Company Profile

SAS Institute Inc. is a privately held, North Carolina, US corporation created in 1976. SAS offers business analytics software and services, delivered to customers throughout the world. Sales activities are conducted primarily through SAS Institute Inc. and its controlled sales subsidiaries in approximately 150 countries. The sales subsidiary entities are grouped into three regional sales divisions: the Americas; Europe, Middle East and Africa (EMEA); and Asia Pacific.

You can learn more about SAS by reading our **Annual Report** and read more about SAS' governance and corporate social responsibility by visiting **Corporate Social Responsibility and Innovation**.

You can also access our **Trust Center** to read more about our commitments to security, privacy and compliance, including white papers about the **SAS Product Security Framework** and the **SAS Quality Imperative**.

SAS Services and the Shared Responsibility Model

Our customers consume SAS software and services in a variety of ways. Allocations of risk and responsibilities vary based on the nature of the service performed. It is important to understand the shared responsibility model relative to risk, including which security tasks are handled by SAS and which tasks are handled by our customers.

Responsibilities vary depending on whether the workload is hosted on customer premises or hosted by SAS in our secure SAS Managed Cloud. In an on-premises environment, security responsibilities are owned by the customer. When SAS provides hosting services, more of the day-to-day security responsibilities move to SAS.

Typical SAS Offerings

On-Premises Software and Technical Support

SAS licenses SAS software to customers for installation in an environment that is owned by the customer or a third party on the customer's behalf (on-premises software).

In connection with on-premises software, SAS provides 24/7 remote technical support services via telephone or email. In these cases, the customer tends to maintain its own administrator of the SAS software and IT support desk and liaises with SAS as needed to resolve issues.

When SAS is problem solving, we often seek to replicate the issue and fix it in our own technical support environment before making our fix suggestion to the customer's support team, who then applies the same fix in their environment. Most technical support issues can, therefore, be resolved remotely, without the need for access to customer systems or data.

In rare cases, SAS and our customer may agree that resolution can be expedited by holding a video conference call where the customer shows SAS on-screen what is happening in its environment when an issue arises, or by sharing data with SAS, such as log files containing IP addresses. In these cases, it is possible that SAS may have limited access to customer data, which may include personal data, as defined by applicable privacy laws. The customer notifies SAS before sharing such data so that an assessment of necessity, scope and purpose is completed before such access occurs.

SAS offers both Standard and Premium Technical Support using the same general engagement model described above. You can learn more at **SAS Support Services** and read about the standard support policies, including **support levels and target response times**.

SAS Managed Cloud Services

SAS can help customers realize the full value of digital transformation with a comprehensive range of SAS Managed Cloud Services offerings and deployment patterns. The **SAS Cloud Executive Summary** provides an initial overview of our offerings.

Hosted Managed Services

SAS offers Hosted Managed Services as a SAS Managed Cloud Services offering option for customers looking for a comprehensive solution based on SAS' industry-leading analytics products – offerings delivered by SAS. Hosted Managed Services are housed in any of the SAS Managed Cloud Services hosting centers or selected cloud providers (such as Microsoft Azure or Amazon Web Services, depending on the specific service provision) across the globe.

You can read more about Hosted Managed Services in our **service brief** and **white paper**. Details of the standard services, and roles and responsibilities, are also described in the **RACI Matrix**.

Remote Managed Services

One of our SAS Managed Cloud Services offerings, SAS Remote Managed Services, meets customers' application management needs when customers require or prefer that the software solution and data remain on the customer's premises (or within their third-party hosted data center).

Customers provide all necessary infrastructure to operate and maintain the SAS solution in their data center. SAS Remote Managed Services provide remote monitoring and technical management of SAS software applications. This service allows customers to fully capitalize on the skill, knowledge and expertise of SAS resources. The offering may include service operations management; SAS application management; capacity planning; and event, incident and problem management within the defined service-level agreements.

Before these services begin, the teams review and understand the customer's security policies applicable to its data center to ensure that the SAS team can follow these policies in full.

You can read more about SAS Remote Managed Services in our **service brief** and **white paper**.

SAS Training and Education

SAS also offers training courses about SAS Software. Customer data and access to customer systems is not required for the provision of training courses.

Professional Services

SAS offers consulting services to help customers implement SAS software. SAS will comply with relevant customer policies while performing services on customer premises or within its systems.

In many cases, consulting services can be performed without access to (personal) data. SAS will not receive (personal) data unless it is necessary to perform our services. SAS professional services teams work with our customers to restrict and control access to data to ensure personal information is only accessible to those that absolutely require it.

Customer Contact Information

When a customer's employees interact with SAS – such as when contacting technical support, inquiring about software or services, or attending training courses – SAS may collect certain administrative information such as the employee's name and contact information. SAS protects that information in accordance with our Privacy Policy (available at SAS' Trust Center – **SAS Privacy Statement**) and applicable law. When acting as a data processor, we enter into data processing agreements with customers based on the **SAS Data Processing Agreement**.

Overview of the APRA CPS 230 Standard

APRA CPS 230 Objectives

A key objective of the Australian Prudential Regulation Authority (**APRA**) is to ensure that financial services organizations manage operational risk. More specifically, CPS 230 requires APRA-regulated entities:

- To strengthen operational risk management by addressing identified weaknesses in existing controls and enhance third-party risk management by managing risks from material service providers.

- To the extent practicable, minimize disruption to essential operations and resume normal operations promptly after a disruption ends.
- To maintain a comprehensive service provider management policy, and a register of material services providers, as well as negotiate license agreements with relevant terms.
- To develop and maintain business continuity plans, which set out how to identify, manage and respond to disruption.

APRA recently issued Prudential Standard **CPS 230** to replace the current APRA Prudential Standards for Outsourcing (CPS 231 / SPS 231 / HPS 231) and Business Continuity Planning (CPS 232 / SPS 232). CPS 230 will become the standard for APRA-regulated entities when outsourcing services and managing operational risk. The effective date for the standard is 1 July 2025. For preexisting contractual arrangements with service providers, the standard will only apply from the next contract renewal date or 1 July 2026, whichever comes first.

To assist customers meeting the requirements imposed on them under CPS 230, SAS maintains a number of security and privacy certifications for its operations. These provide assurance to our customers that SAS takes the security and resilience of the processing of customers' data, either by the customer on-premises or as a managed service, very seriously.

Minimum Terms for APRA-Regulated Financial Institutions

In service provider arrangements, CPS 230 focuses on the operational risks that arise from services provided to financial institutions, especially by Material Service Providers. CPS 230 defines a Material Service Provider as one that the institution relies on for a "Critical Operation" or that exposes them to significant operational risk. A Critical Operation is defined as processes that, if disrupted beyond acceptable levels, would significantly impact depositors, policyholders, beneficiaries, other customers or the financial system role of the APRA-regulated entity.

SAS' Assurance Response

To assist customers meeting the requirements imposed on them under the various directives and regulations, including APRA CPS 230, SAS maintains several security and privacy certifications for its operations (such as ISO 27001). For further details, please see the **SAS Trust Center**.

SAS is committed to facilitating our customers' compliance with these regulatory requirements by helping to convey how SAS, as a service provider, might expose a financial institution to risk, and any areas where SAS can help mitigate that risk. CPS 230 breaks down its directives into several primary categories. In general terms, SAS seeks to provide:

1. Clarity about the nature of our services.
2. Confidence that there will be continuity of service.
3. Transparency, including commitments to security and business continuity.

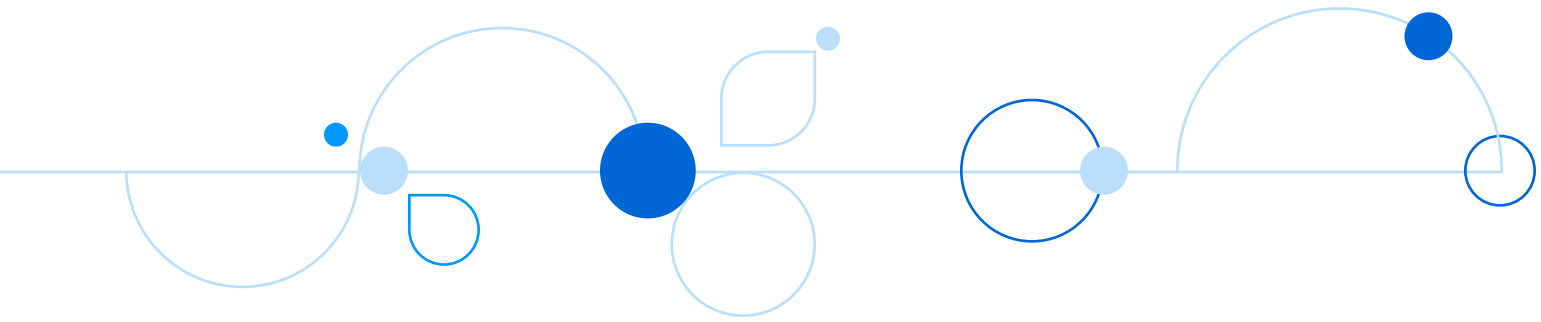
The table that follows seeks to provide assurance that SAS' security controls and practices will help our financial services customers meet their CPS 230 obligations as they apply to SAS, as a service provider under the shared responsibility model.

APRA-Regulated Entity Category Requirements	SAS' Assurance Response
Operational Risk Management Framework & Governance	**APRA CPS 230 requirement** APRA mandates that financial services firms ensure proper governance and oversight of operational risk programs. This includes defining risk appetite and tolerance; monitoring, analyzing and reporting operational risks; and escalating incidents to the Board. **SAS' assurance response** SAS, as a software and hosting management services provider, partners with customers to provide information that would factor into a financial institution's operational risk assessment, including confirmation of SAS' governance activities. This involves details and evidence of SAS' applicable security certifications (e.g., ISO 27001, SOC 2 Type II) as well as details of SAS' **Technical and Organizational Security Measures** (TOMs) related to SAS Managed Cloud Services. SAS' TOMs include areas such as security practices, network security, email security, logical access, physical security, personnel security, operational and security incident response practices, and data destruction requirements. TOMs operate to provide applicable controls relating to the availability, authenticity, integrity and confidentiality in relation to the protection of data, including personal data. Likewise, for SAS on-premises arrangements, SAS offers the **SAS Quality Imperative**. This document describes detailed and technical processes that are used in SAS' software development, including security testing, deployment and maintenance/support. In addition, various types of internal assessments of risk are conducted by SAS at least annually to identify scenarios within SAS where risks could exist or arise at a given time. Risk assessments may be conducted at the organization level, mission/business process level and/or information system level. As an example, SAS performs its own annual information security risk assessment of SAS' managed and hosted customer environments, including third-party cloud service provider environments, using a recognized standard and framework (e.g., NIST 800-30). With respect to incident management, SAS maintains incident management policies and processes to ensure the rapid detection and restoration of services that can occur from incidents that affect, or have the potential to affect, SAS' managed and hosted customer environments, including third-party colocation data centers or third-party cloud service providers. Processes provide the following, when appropriate: • Initial assessment of the extent, severity and impact of an incident. • Resource coordination. • Status communication and reporting to internal and external stakeholders. • Information gathering and fact finding, including, but not limited to, defect recording, hot fix determination and identification of service improvement initiatives. • Action prioritization to recover from the incident or event. • Post-incident documentation and communication. For customers who license SAS software for deployment and use on their own systems, notifications are published on our support site at **sas.com/support**.

APRA-Regulated Entity Category Requirements	SAS' Assurance Response
Operational Risk Profiles, Assessments, Controls and Incidents	**APRA CPS 230 requirement** APRA-regulated financial institutions must sustain critical operations and manage risks effectively. This involves monitoring IT solutions' health, informing the Board and senior management of their status, documenting IT solutions, analyzing and testing risk impacts, and implementing measures to reduce and report on operational risks. **SAS' assurance response** SAS, as a software and hosting management services provider, provides information to its customers that would factor into a financial institution's operational risk assessment. This includes compliance reporting of applicable security certifications (e.g., ISO 27001) as well as details of SAS' **Technical and Organizational Security Measures** related to SAS Managed Cloud Services. The SAS Security Governance Manual (SGM), available with an NDA in place, also provides details regarding our team's roles and responsibilities, SAS' operational processes, and our security controls. SGM topics include, but are not limited to: • Network boundary protections, including perimeter security and malicious code protection monitoring. • Configuration management, including use of configuration baselines (e.g., Center for Internet Security (CIS)). • Change management practices and reporting. • Vulnerability testing and reporting. • Audit logging and monitoring. Regarding operational performance and related metrics requirements, SAS monitors server health and captures metrics of cluster, server and solution availability, which may involve: • Server uptime. • Disk usage per file system. • List of user IDs that are currently logged onto the server. • Network interface status. • Total disk usage. • Completion of successful backups. • CPU specifications. • Memory utilization. For on-premises solutions, SAS provides Technical Support response metrics, which may include: • Initial response timing. • Ongoing response/comments timing. • Timing of resolution/closure. Additional metrics may also be made available via SAS' Enhanced Support Offerings of technical support case details (e.g., number, software type, timing, environment involved, etc.). The SGM also offers details about our SAS Solution Delivery Methodology (SDM), including SAS project phases (e.g., definition, design, build, test, implementation and maintenance) and related deliverables. For SAS on-premises arrangements, SAS offers the SAS Quality Imperative. This document describes SAS' software development, including security testing, deployment and maintenance/support.

APRA-Regulated Entity Category Requirements	SAS' Assurance Response
Business Continuity Management (BCM)	**APRA CPS 230 requirement** CPS 230 mandates creating Business Continuity Plans (BCPs) detailing how a financial institution will manage and respond to disruptions affecting people, technology, information, facilities and service providers. These plans must address interdependencies, risks, obligations, key data and controls, and be regularly tested. **SAS' assurance response** The practices and plans under SAS' BCM Program support customer requirements for BCM applied to their SAS solution, whether on-premises or hosted by SAS Managed Cloud Services. SAS' BCM Program, initiated in 2004, undergoes periodic independent review through customer assessments and/or internal audits/assessments in alignment with ISO standards (e.g., ISO 27001 and ISO 22301). SAS' BCM Program is managed by SAS' BCM Program Office under executive sponsorship from the SAS Corporate Services, SAS Legal Services, and SAS CIS divisions. The BCM Program Office staff supports SAS' Business Continuity Management (BCM) program and processes, which formalizes roles and responsibilities and standardizes specific activities that include Business Impact Analysis (BIA), annual plan maintenance and testing, staff training, and management reviews. SAS' BCM Program has responsibility for incident/crisis management plan management activities for SAS' global offices as well as business resumption plan management activities by critical business functions. SAS' global recovery strategies for several key customer-facing functions include: • Communications. • Licensing operations. • Technical support. • Professional services. • SAS Managed Cloud Services. SAS applies an all-hazards business continuity management planning approach to document recovery strategies for the following: • Loss of people (for example, critical function services can be provided from SAS resources in other geographic locations). • Loss of facility (for example, SAS resources can work from alternate locations, including home). • Loss of technology (for example, where appropriate, critical functions utilize manual work-arounds). • Loss of key suppliers or partners (for example, where appropriate, SAS engages alternative suppliers and partners). In addition, SAS' Cloud and Information Services (CIS) Division has responsibility for: • Technology resilience strategies. • Disaster recovery (DR) planning for key infrastructure, such as servers, applications, data stores and communications assets. • Management of security incidents under the Security Incident Response Team (SIRT) Process.

APRA-Regulated Entity Category Requirements	SAS' Assurance Response
Management of Service Providers (Third and Fourth Parties)	**APRA CPS 230 requirement** CPS 230 mandates that APRA-regulated financial institutions manage crucial aspects of their operations, including those handled by key service providers. This involves identifying these providers, overseeing policies and contracts, conducting due diligence, and managing risks that could impact service performance. **SAS' assurance response** The agreements between SAS and our customers include terms that will allow appropriate management by a CPS 230-regulated financial entity of our activities. These terms include rights, responsibilities and expectations of each party to the agreement, including in relation to the ownership of assets, ownership and control of data, dispute resolution, audit terms, termination provisions, liability, and indemnity. SAS maintains a governance and compliance program as well as associated policies to manage our service providers providing services for SAS in support of HMS and RMS offerings. The program includes evaluation of SAS' ongoing third-party service providers' performance and the security posture of the third-party to ensure delivery of services. This involves managing the third-party life cycle, including third-party contracts, information security risk assessments, performance and renewals until the end of the contract. Third parties that provide critical products or services are evaluated/assessed to ensure that they have the appropriate security controls and infrastructures in place. In addition, SAS maintains a due diligence Third-Party Qualification and Information Security Risk Management Program that includes assessment, evaluation, approval, disapproval and continuous improvement of its third-party subcontractor base assigned to projects that access the managed and hosted customer environments, as appropriate. These third parties who provide subcontractors are evaluated/assessed to verify that they maintain data and information security controls, infrastructure, policies and safeguards that meet or exceed SAS' minimum security requirements.



For more information, please visit sas.com.