WHITE PAPER

EU Digital Operational Resilience Act (DORA) Advisory

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 the European Union Digital Operational Resilience Act (DORA) that may impact customer adoption of SAS services.
- A checklist of how SAS helps organizations to remain compliant with those regulations.

This document will be a helpful starting point for EU financial institutions when considering use of SAS services, to conduct an initial risk assessment. The document will reference more detailed documentation that is maintained and updated over time.

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 their 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 managed cloud 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 an 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 data centers or selected third-party cloud service providers (such as Microsoft 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 offerings, SAS Remote Managed Services, meets customers' technical 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 skills, 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 the use of 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 DORA Standard

DORA Objectives

The Digital Operational Resilience Act (DORA) is a European Union (EU) regulation that creates a comprehensive information and communication technology (ICT) risk management framework for the financial sector within the EU. More specifically, DORA establishes standards that apply to financial institutions, including banks, insurance companies and investment firms, and their "critical" third-party technology service providers. DORA has three main objectives:

1. To comprehensively address ICT risk management in the financial services sector.
2. To harmonize the ICT risk management regulations that already exist in individual EU member states.
3. To strengthen the IT security of EU financial entities to best ensure that the financial sector is resilient in the event of a severe operational disruption.

DORA Scope

DORA covers multiple areas related to the security of ICT systems supporting business processes for financial institutions:

- Risk management governance.
- Incident classification and reporting.
- Digital operational resilience testing/business continuity management.
- Third-party risk management.
- Critical service provider oversight.

DORA's technical standards that apply to financial entities and their critical third-party technology service providers must be implemented by 17 January 2025.

DORA Enforcement

Enforcement of DORA will be the responsibility of designated regulators in each EU member state, known as "Competent Authorities." These Competent Authorities will play a critical role in enforcing security measures. They have the authority to both request specific actions from DORA-regulated financial entities and to impose penalties, which can include administrative or criminal sanctions determined by each member state.

For ICT providers deemed "critical," direct supervision by "Lead Overseers" from the European Supervisory Authorities (ESAs) adds another layer of oversight. Similarly to Competent Authorities, Lead Overseers also can request security measures and remediation efforts. In addition, they have the authority to impose fines directly on ICT providers amounting to 1% of the provider's average daily worldwide turnover in the previous business year. Critical ICT Providers can be fined every day for up to six months until they achieve compliance.

SAS' Assurance Response

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

SAS is committed to facilitating 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. In general terms, SAS seeks to provide:

- Clarity about the nature of our services.
- Confidence that there will be continuity of service.
- 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 DORA obligations as they apply to SAS, as an ICT provider under the shared responsibility model.

DORA-Regulated Entity Category Requirements	SAS' Assurance Response
Risk Management, Data and Security	**DORA requirement** DORA stipulates requirements for financial services organizations that include governance and oversight of risk programs. The financial entity's management is fully accountable for the management of ICT risks, for setting and approving its digital operational resilience strategy, and for reviewing and approving policies regarding the use of ICT third-party providers (TPPs). It also requires the development of risk tolerances for ICT disruptions supported by metrics. Financial entities must identify their "Critical or Important Functions" (CIFs) and map their interconnections between ICT assets, processes and systems. In addition, financial entities are required to implement ICT security practices that help ensure the resilience, continuity and availability of ICT systems, for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data. **SAS' assurance response** SAS, as a provider of software and hosted managed services, partners with customers to provide information that would factor into a financial institution's ICT risk assessment and its mapping of SAS solution assets, processes and systems. This includes compliance reporting of 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. TOMs include 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. SAS Cloud Information Services (CIS) policies and processes are managed through SAS' Quality Management System/Information Security Management System (QMS/ISMS) Board. The SAS Security Governance Manual (SGM), available to customers with an NDA in place, is updated annually and approved by the QMS/ISMS Board. The document sets forth policies and processes to enable adequate safeguards to protect the confidentiality, integrity and availability of data. The SGM provides details regarding SAS' security roles and responsibilities as well as SAS' operational processes. Topics include those that are associated with our SAS Managed Cloud solution health, such as, but not limited to: • Account management and access control, including on-off-boarding. • Network boundary protections, including perimeter security and malicious code protection monitoring. • Data loss prevention management. • Vulnerability management. • Audit logging and monitoring. • Availability monitoring and event management. • Incident management reporting. • Change management. • Risk management and reporting.

DORA-Regulated Entity Category Requirements	SAS' Assurance Response
	In addition, the SGM offers details about our SAS Solution Delivery Methodology (SDM) applied under a respective consulting agreement, including SAS project phases and related deliverables that are specific to a customer's solution. With respect to SAS' risk programs, 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/ISO 27005). 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. SAS Cloud Services Delivery Managers work with SAS Managed Cloud Services customers directly to execute a project-focused risk assessment. For any project, a risk is defined as any event likely to adversely affect the successful completion of the project. This process ensures each risk identified within the project environment is documented, categorized and addressed in the most appropriate manner. Risks may develop as the project matures as both internal (project team resources) and external (customer) factors influence the project. All risks are tracked through closure using an automated ticketing system. SAS' customers are involved in all stages of this process by reporting, reviewing and providing input into external (customer) risk results. The project risk management process involves the following key stages: • **Risk identification:** This step involves identifying and classifying vulnerabilities and risks. • **Risk assessment:** Once risks are identified, the next step is to analyze each risk within the context of its consequence (impact) and likelihood of occurring (probability). SAS then uses a semiquantitative rating to score the risk as high, medium or low. • **Risk response planning and execution:** Risk planning is the function of deciding what actions, if any, should be taken in response to each risk. At a minimum, risk response plans should be developed for those risks with high-risk scores. Risk treatment actions include mitigation, transfer and acceptance. The SAS project team and the customer review and/or reassess risks on a periodic basis, as appropriate. Updates are made as needed to the identified risks until they are fully addressed and then closed.

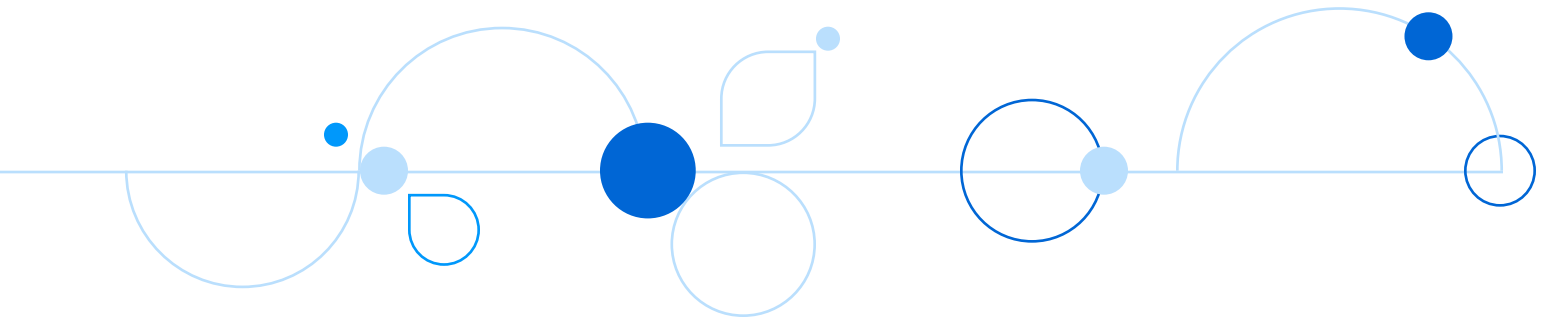
DORA-Regulated Entity Category Requirements	SAS' Assurance Response
Incident Classification and Reporting	**DORA requirement** DORA requires financial institutions to follow an incident classification, notification and reporting framework that includes collection, analysis, escalation and reporting of ICT incidents and threats. As applicable, assessment requirements include services affected, duration of downtime, geographical spread, data loss, economic impact and reputational impact. Where applicable, thresholds must be determined in the impact analysis. **SAS' assurance response** SAS, as an ICT provider, provides incident management process documentation and applicable incident details to financial institutions to factor into their incident analysis and reporting requirements. 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. In the event that SAS only provides a license to SAS software for deployment and use on customers' systems, notifications are published on our support site at **sas.com/support**.

DORA-Regulated Entity Category Requirements	SAS' Assurance Response
Business Continuity Management (BCM)	**DORA requirement** DORA requires the development of Business Continuity Plans (BCPs) that specify how the financial institution would identify, manage and respond to a disruption within tolerance levels including people, technology, information, facilities and service providers, the interdependencies across them, and the associated risks, obligations, key data and controls. In addition, the plans must 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 in the SAS Managed Cloud and managed by SAS. 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. 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. 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).

DORA-Regulated Entity Category Requirements	SAS' Assurance Response
Management of Service Providers/ Subcontracting	**DORA requirement** Regulated financial institutions are required to manage their critical operations, including those managed by its service providers. This includes identification of service providers, and management of associated policies and contract terms. Appropriate due diligence in the assessment phase is required, along with identification and management of risks that could affect the ability of the service provider to perform the service on an ongoing basis. **SAS' assurance response** The agreements between SAS and our customers include terms that allow appropriate management of activities. These terms include rights, responsibilities and expectations of each party to the agreement, such as in relation to the ownership of assets, rights to and control of data, dispute resolution, audit terms, exit planning and termination provisions, liability, and indemnity. SAS maintains a governance and compliance program and policies to manage our own service providers providing services for SAS, including SAS Managed Cloud Services. 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 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. Third-party agencies who provide subcontractors are evaluated/assessed to that they maintain data and information security controls, infrastructures, policies and safeguards that meet or exceed SAS' minimum security requirements.

DORA-Regulated Entity Category Requirements	SAS' Assurance Response
Vulnerability Management	**DORA requirement** DORA requires that financial institutions adequately manage vulnerabilities and/or requires their ICT service providers manage vulnerabilities that may affect critical or important processing carried out by them. Vulnerability management procedures should track the usage of third-party software libraries, including open source, used by ICT services supporting a critical or important function. **SAS' assurance response** SAS performs vulnerability management processes for SAS-managed systems, including technical vulnerability identification, evaluation and correction. All vulnerability scanners are configured to update automatically when new signatures are available. Before a vulnerability scan is conducted, the SAS Global Information Security (GIS) resources conducting the scan ensure that the vulnerability scanner is performing a scan using the most current, up-to-date inventory. SAS ensures that internet-facing applications that store, process or transmit restricted or confidential customer data undergo automated vulnerability testing monthly. SAS also reviews security alerts, vulnerabilities, etc., on a daily basis. Vulnerability scan data is aggregated, analyzed and risk assessed by SAS GIS to determine and compare vulnerability trends as applicable. SAS' risk assessment includes the Common Vulnerability Scoring System (CVSS) criticality rating and considers the availability of a system (i.e., internal vs. external), whether the vulnerability is exploitable, and the type of data on the system(s) in question. If this review identifies that the vulnerability has been exploited, appropriate actions are taken to investigate the incident and remediate the identified vulnerability. SAS also assesses the impact of this information and findings with SAS system owners/system administrators. SAS also performs regular patching of devices to keep OS and third-party software up to date. Various teams are responsible for monitoring and evaluating security bulletins and patch releases from vendors to determine if these patches are appropriate. SAS annually performs independent network penetration tests of its SAS Managed Cloud in accordance with recognized testing standards. SAS, on a confidential basis, will provide the customer at its written request a letter of attestation that includes scope and methodology of such tests. When requested by a customer, SAS will participate and cooperate in the process of a threat-led penetration test in accordance with regulatory requirements under DORA and subject to mutually agreed processes. For on-premises customers, financial entities are required to execute the test in their own production environments. SAS will help facilitate issues management through our Technical Support processes. For customers hosted in the SAS Managed Cloud, SAS will permit the customer to conduct a penetration test subject to rules that maintain security and confidentiality of our other SAS Managed Cloud Services customers.

DORA-Regulated Entity Category Requirements	SAS' Assurance Response
Monitoring of ICT Service Provider	**DORA requirement** DORA requires effective monitoring and reporting obligations of ICT third-party service providers to the financial entity, including notification of any event or disruption that might have a material impact on the ICT third-party service provider's ability to effectively provide services. **SAS' assurance response** Regarding operational performance and related metrics requirements for the SAS Managed Cloud, SAS monitors server health and captures metrics of cluster, server and solution availability, such as the following: • Server uptime. • Disk usage per file system and total disk usage. • Network interface status. • Completion of successful backups. • CPU specifications. • Memory utilization. Regular reviews of operational cloud service health metrics are facilitated by SAS Managed Cloud Services teams. Regarding operational metrics for on-premises solutions, SAS provides Technical Support response metrics. Target response times are provided for initial follow-up of support requests and for frequency of updates according to severity. Additional metrics may also be made available via Premium Support, which offers an assigned Technical Support Account Manager (TSAM) and a reporting portal. TSAMs provide proactive technical advice and guidance and facilitate regular reviews of metrics and status of customer-specific Technical Support activity. For more information please see **SAS' Technical Support area** and the **Premium Technical Support page**.



For more information, please visit sas.com.