WHITE PAPER

Contract Checklist for the EU Digital Operational Resilience Act (DORA)

Contents

Disclaimer
The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation, or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their use of SAS services. Please also note that the relevant contract(s) between you and SAS determine(s) the scope of services provided and the related legal terms and this document is provided for reference purposes only, and is not part of, and does not otherwise create or amend, any agreement, warranties, representations or other obligations between you and SAS. SAS disclaims any terms or statements contained herein that seek to impose legal or operational requirements on SAS for the delivery of the services. Customers acknowledge that they remain solely responsible for meeting their legal and regulatory requirements.

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

Introduction

SAS has created this document to help our financial services customers operating in the European Union (EU) assess the use of SAS services in light of the Digital Operational Resilience Act (DORA). As we understand the challenges that come along with the implementation of DORA, we want to make it easier for our financial services customers to identify the sections of the SAS standard agreements that may support them in addressing the applicable DORA requirements.

Regulatory Background

DORA forms part of the digital finance strategy adopted by the European Commission in 2020. It aims to establish a harmonized regulatory framework on digital operational resilience for financial entities operating in the EU. Its objectives include ensuring that financial entities can withstand, respond to and recover from information and communication technology (ICT)-related disruptions and threats, such as cyber threats. DORA applies to all authorized financial entities operating in the EU, subject to limited exceptions. It also creates an oversight framework for ICT third-party service providers to the financial sector that are deemed critical.

As a regulation, DORA is directly legally binding in all EU member states. It entered into force on 16 January 2023, and its provisions apply from 17 January 2025 following a 24-month implementation period.

This document completes the *SAS EU DORA Advisory* white paper.

The SAS agreement includes the following customer-specific components, which are referenced in this document:

- Order Form (UTOF) – specified/individualized to the agreed services in scope, and attached to it, standardised:
  - Universal terms and the relevant service-specific addenda.
  - Data Processing Addendum (“DPA”) as applicable.
  - Addendum for Regulated Customers as applicable.

For more information on how to contract with SAS, please visit the SAS website **Contracting With SAS**.

In this document, financial services customers will find a list of contractual requirements under DORA, along with references to the relevant documents of SAS and a short explanation to help them conduct their internal review of SAS agreements.

Assessment Matrix

Article	Requirement	Referenced SAS Documents	SAS Comments
Managing of ICT Third-Party Risk. General Principles (Articles 28 and 29 of DORA).			
28.3	As part of their ICT risk management framework, **financial entities (SAS customers) shall maintain and update** at entity level, and at subconsolidated and consolidated levels, **a register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers**.	• Art. 3.1 Addendum for Regulated Customers. • Information on SAS EU Companies and Contact Details can be found here: **https://www.sas.com/en_gb/legal/privacy/eu-contacts.html**.	Maintaining a register of information is financial entity's internal obligation. SAS contractual documentation and the information provided on SAS websites allow its customers to complete the register. However, upon reasonable request, SAS will provide its Customers with additional information helping them to maintain and update the information register in compliance with DORA.
28.4	Before entering into a contractual arrangement on the use of ICT services, financial entities shall: a. Assess whether the contractual arrangement covers the use of ICT services supporting a critical or important function; b. Assess if supervisory conditions for contracting are met; c. Identify and assess all relevant risks in relation to the contractual arrangement, including the possibility that such contractual arrangement may contribute to reinforcing ICT concentration risk as referred to in Article 29; d. Undertake all due diligence on prospective ICT third-party service providers and ensure throughout the selection and assessment processes that the ICT third-party service provider is suitable; e. Identify and assess conflicts of interest that the contractual arrangement may cause.	Please review our terms at: **Contracting With SAS**.	To support Customers in their efforts to meet their obligations under Art. 28(4) DORA, SAS publishes information about its commitments related to security, privacy, compliance and quality on the SAS Trust Center website: **https://www.sas.com/en_us/trust-center.html**. All SAS terms are available for Customers' review at: **Contracting With SAS**.

Article	Requirement	Referenced SAS Documents	SAS Comments
28.5	Financial entities may only enter into contractual arrangements with ICT third-party service providers that comply with appropriate information security standards. When those contractual arrangements concern critical or important functions, financial entities shall, prior to concluding the arrangements, take due consideration of the use, by ICT third-party service providers, of the most up-to-date and highest quality information security standards.	• Art. 7.1 – 7.3 Addendum for Regulated Customers. • Art. 13 and 14 Universal Terms. • Schedule 2 to the SAS DPA. • Art. 12 Hosted Managed Services Addendum.	The Customer may find more information on SAS' commitments to security on the SAS Trust Center website **https://www.sas.com/en_us/trust-center.html**, and in particular on the subpages related to the **SAS Product Security Framework** and the **SAS Quality Imperative**.
28.7	Financial entities shall ensure that contractual arrangements on the use of ICT services may be terminated in any of the following circumstances: a. Significant breach by the ICT third-party service provider of applicable laws, regulations or contractual terms; b. Circumstances identified throughout the monitoring of ICT third-party risk that are deemed capable of altering the performance of the functions provided through the contractual arrangement, including material changes that affect the arrangement or the situation of the ICT third-party service provider; c. ICT third-party service provider's evidenced weaknesses pertaining to its overall ICT risk management and in particular in the way it ensures the availability, authenticity, integrity and confidentiality of data, whether personal or otherwise sensitive data, or nonpersonal data; d. Where the competent authority can no longer effectively supervise the financial entity as a result of the conditions of, or circumstances related to, the respective contractual arrangement.	• Art. 8. Addendum for Regulated Customers. • Art. 2.2 Universal Terms. • Art. 16 Hosted Managed Services Addendum.	Please see the section referring to Art. 30.2 (h) DORA below.

Article	Requirement	Referenced SAS Documents	SAS Comments
28.8	For ICT services supporting critical or important functions, financial entities shall put in place exit strategies. The exit strategies shall take into account risks that may emerge at the level of ICT third-party service providers, in particular a possible failure on their part, a deterioration of the quality of the ICT services provided, any business disruption due to inappropriate or failed provision of ICT services or any material risk arising in relation to the appropriate and continuous deployment of the respective ICT service, or the termination of contractual arrangements with ICT third-party service providers under any of the circumstances listed in paragraph 7. Financial entities shall ensure that they are able to exit contractual arrangements without: a. Disruption to their business activities, b. Limiting compliance with regulatory requirements, c. Detriment to the continuity and quality of services provided to clients. Financial entities shall identify alternative solutions and develop transition plans enabling them to remove the contracted ICT services and the relevant data from the ICT third-party service provider and to securely and integrally transfer them to alternative providers or reincorporate them in-house. Financial entities shall have appropriate contingency measures in place to maintain business continuity in the event of the circumstances referred to in the first subparagraph.	• Art. 9 Addendum for Regulated Customers.	Please see the section referring to Art. 30.3 (f) DORA below.

Article	Requirement	Referenced SAS Documents	SAS Comments
KEY CONTRACTUAL PROVISIONS UNDER DORA ARTICLE 30			
30.1 DORA	The **rights and obligations** of the financial entity and of the ICT third-party service provider **shall be clearly allocated and set out in writing**.	• All SAS Agreements are in writing (**Contracting With SAS**). • Individual Order Form for the relevant SAS Offering with attached terms, including the Addendum for Regulated Customers.	The parties' rights and obligations are stipulated in the individual Order Forms, which refer to the Universal Terms and to the relevant addenda, including the Addendum for Regulated Customers. A detailed description of the parties' Hosted Managed Services activities is set forth in the RACI document available under section 1 of the SAS Hosted Managed Services Addendum (**https://www.sas.com/raci**). All SAS Agreements are in writing (**Contracting With SAS**).
30.1 DORA	The full contract shall **include the service level agreements**.	Service Level descriptions are detailed in the relevant addenda: Please refer to the relevant Service Level Warranty Addendum **here**.	SAS contractual documents, including Service Level Warranty Addenda, provide for specific service level descriptions that SAS commits to in relation to its Customers. Those descriptions include performance metrics allowing Customers to effectively monitor and measure SAS' performance.
30.1 DORA	The full contract shall be documented in **one written document**, which shall be available to the parties on paper, or in a document with another downloadable, durable and accessible format.	• Individual Order Form for the relevant SAS Offering contains active referral to all applicable documents.	Agreements between SAS and its Customers are usually signed via Docusign. Once the contractual documents are signed, they are available to Customers in a downloadable format. In addition, SAS keeps track of all updates to its contractual documentation: **https://www.sas.com/contract-with-sas-archive**.

Article	Requirement	Referenced SAS Documents	SAS Comments
30.2.a DORA	The contractual arrangements on the use of ICT services shall include **a clear and complete description of all functions and ICT services to be provided** by the ICT third-party service provider, **indicating whether subcontracting** of an ICT service supporting a critical or important function, or material parts thereof, **is permitted** and, when that is the case, **the conditions applying to such subcontracting**.	• Individual Order Form for the relevant SAS Offering. • Relevant documentation for the respective service. • Art. 5 Addendum for Regulated Customers.	Agreements between SAS and its Customers, in particular Order Forms and service-specific addenda and documentation, include comprehensive descriptions of SAS services. Art. 5 of the Addendum for Regulated Customers sets out the rules governing the subcontracting of SAS services as required under DORA and as necessary to maintain the highest level of service security and quality.
30.2.b DORA	The contractual arrangements on the use of ICT services shall include the **locations**, namely the regions or countries, **where the contracted or subcontracted functions and ICT services are to be provided and where data is to be processed**, including the storage location, **and the requirement for the ICT third-party service provider to notify the financial entity in advance if it envisages changing such locations**.	• Individual Order Form for the relevant SAS Offering. • Art. 6 Addendum for Regulated Customers.	At a Customer's request for Hosted Managed Services, SAS is able to provide Hosted Managed Services with limited data access (Data Protection and EU Data Boundary Principles), and SAS will provide a cloud environment located in the European Economic Area/United Kingdom (EEA/UK). Upon agreement, the Order Form includes wording that references the EU Data Boundary Principle as applied by SAS.

Article	Requirement	Referenced SAS Documents	SAS Comments
30.2.c DORA	The contractual arrangements on the use of ICT services shall include **provisions on availability, authenticity, integrity and confidentiality** in relation to the protection of data, including personal data.	• Art. 13, 14 Universal Terms. • DPA. • Art. 12 Hosted Managed Services Addendum. • Art. 7 Addendum for Regulated Customers.	The availability, authenticity, integrity and confidentiality of Customers' data constitute a vital element of SAS' strategy regarding the security of services. In addition to the confidentiality obligations included in the Universal Terms, the data availability levels addressed in the relevant service level provisions, and the security measures referred to in the SAS DPA and the Addendum for Regulated Customers, SAS publishes its commitments to maintaining high security standards on the SAS Trust Center website **https://www.sas.com/en_us/trust-center.html**.
30.2.d DORA	The contractual arrangements on the use of ICT services shall include provisions on **ensuring access, recovery and return** in an easily accessible format of **personal and nonpersonal data** processed by the financial entity in the event of the **insolvency, resolution or discontinuation of the business operations** of the ICT third-party service provider, or in the event of the **termination** of the contractual arrangements.	• Art. 9.4 Addendum for Regulated Customers. • Art. 9 of the SAS DPA.	Data retrieval is part of the exit assistance that SAS is ready to provide to its Customers under Art. 9 of the Addendum for Regulated Customers. Specific terms regulating the return of personal data apply in the event that SAS processes personal data on behalf of its Customers. For more information, please see Art. 9 of the SAS DPA.
30.2.e DORA	The contractual arrangements on the use of ICT services shall include **service level descriptions, including updates and revisions** thereof.	• Service Level Warranty Addendum available **here**.	SAS contractual documents, including Service Level Warranty Addenda, provide for specific service level descriptions that SAS commits to in relation to its Customers. Those descriptions include performance metrics allowing Customers to effectively monitor and measure SAS' performance.

Article	Requirement	Referenced SAS Documents	SAS Comments
30.2.f DORA	The contractual arrangements on the use of ICT services shall include the **obligation of the ICT third-party service provider to provide assistance to the financial entity at no additional cost, or at a cost that is determined ex-ante, when an ICT incident** that is related to the ICT service provided to the financial entity occurs.	• Art. 3.4 Addendum for Regulated Customers.	ICT incidents may occur in many different forms and may have different consequences for different entities. SAS is committed to providing its customers with assistance to help them best respond to an incident and quickly restore normal operations. SAS' general obligations in this regard are set out in Article 3.4 of the Addendum for Regulated Customers. They reflect the scope of assistance that SAS may provide to its Customers at any time and at no additional cost. Subject to an additional agreement, SAS may also provide its Customers with additional assistance (professional services) customized to particular customer needs and relating to a specific ICT incident.

Article	Requirement	Referenced SAS Documents	SAS Comments
30.2.g DORA	The contractual arrangements on the use of ICT services shall include the **obligation** of the ICT third-party service provider to fully **cooperate with the competent authorities and the resolution authorities of the financial entity**, including persons appointed by them.	• Art. 3.2 Addendum for Regulated Customers.	SAS services and solutions have supported the financial sector for many years, including central banks that are regulators. SAS fully understands the important role played by financial supervision authorities and other competent authorities for the stability and safety of the sector. SAS, therefore, cooperates with Customers' regulators to the extent reasonably expected under the applicable regulations. SAS is always committed to supporting its financial sector Customers in meeting their regulatory requirements.
30.2.h DORA	The contractual arrangements on the use of ICT services shall include the **termination rights and related minimum notice periods for the termination of the contractual arrangements, in accordance with the expectations of competent authorities and resolution authorities**.	• Art. 8 Addendum for Regulated Customers. • Art. 2.2 Universal Terms. • Art. 16 Hosted Managed Services Addendum.	SAS contractual documents, including the Universal Terms, Order Forms and the Addenda referenced there, grant SAS Customers early termination rights in the event of a material breach by SAS of its obligations. The Addendum for Regulated Customers supplements the above-mentioned early termination rights and grants SAS Customers from the financial sectors additional rights of early termination in cases as provided for in Art. 28.7 DORA.

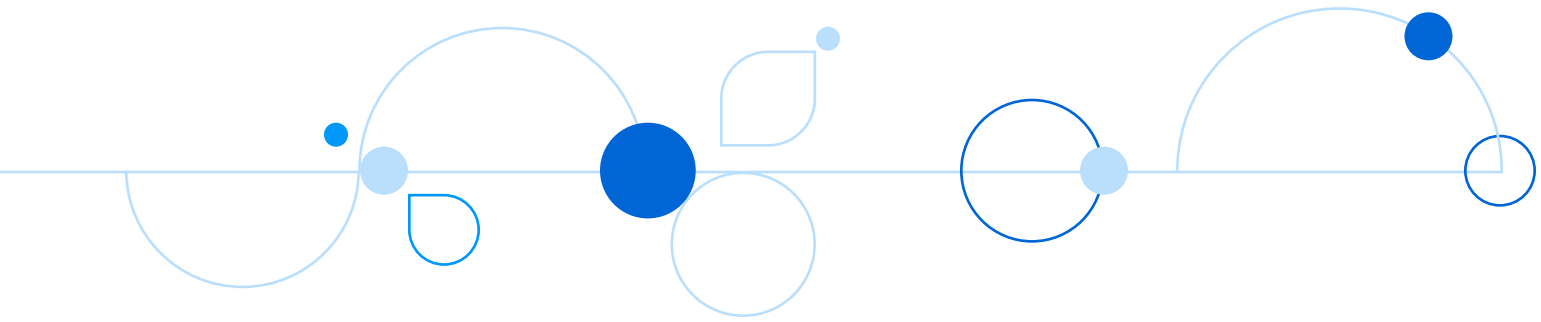
Article	Requirement	Referenced SAS Documents	SAS Comments
30.2.i DORA	The contractual arrangements on the use of ICT services shall include the conditions for the **participation of ICT third-party service providers in the financial entities' ICT security awareness programs and digital operational resilience training** in accordance with Article 13(6).	• Art. 3.6 Addendum for Regulated Customers.	Every member of SAS' personnel is periodically trained in relation to the information security and relevant standards and procedures applicable in the SAS organization. If, in particular situations, SAS financial Customers have specific regulatory needs in relation to training SAS personnel (for example, SAS personnel accessing Customer's premises or ICT environments), SAS is willing to allow its personnel to participate in such Customers' security trainings and awareness programs to the extent these do not have an adverse impact on SAS' business operations.
30.3.a DORA	The contractual arrangements on the use of ICT services supporting critical or important functions shall include **full-service level descriptions**, including **updates and revisions** thereof **with precise quantitative and qualitative performance targets within the agreed service levels** to allow effective monitoring by the financial entity of ICT services and **enable appropriate corrective actions to be taken, without undue delay, when agreed service levels are not met**.	A Service Level description is detailed in the relevant SAS addenda: • Service Level Warranty addendum available **here**.	SAS contractual documents, including the Service Level Warranty Addenda, provide for specific service level descriptions that SAS commits to in relation to its Customers. Those descriptions include performance metrics allowing Customers to effectively monitor and measure SAS' performance. Customers have the possibility of subscribing to an Enhanced/Premium Support service to benefit from additional reports. For more information on this service, **please click here**.

Article	Requirement	Referenced SAS Documents	SAS Comments
30.3.b DORA	The contractual arrangements on the use of ICT services supporting critical or important functions shall include **notice periods and reporting obligations of the ICT third-party service provider to the financial entity**, including notification of **any development that might have a material impact** on the ICT third-party service provider's ability to effectively provide the ICT services supporting critical or important functions in line with agreed service levels.	• Art. 3.3 Addendum for Regulated Customers.	SAS will promptly notify its Customers about material issues impacting the Services, via its standard security reporting processes. Customers have the possibility of subscribing to an Enhanced/Premium Support service to benefit from additional reports. For more information on this service, **please click here**. For more information, please refer to the SAS white paper "DORA Advisory White Paper" for more information.
30.3.c DORA	The contractual arrangements on the use of ICT services supporting critical or important functions shall include requirements for the **ICT third-party service provider to implement and test business contingency plans and to have in place ICT security measures, tools and policies that provide an appropriate level of security** for the provision of services by the financial entity in line with its regulatory framework.	• Art. 4 Addendum for Regulated Customers. • Art. 7.1 – 7.3 Addendum for Regulated Customers.	SAS continues to maintain and test its BCM Program and shares relevant information with its Customers. SAS seeks to address all reasonable concerns of its Customers and is open to discussion in this respect. For more information, please refer to the SAS white paper *EU DORA Advisory*. For additional information regarding SAS' BCM Program, please refer to the ***Business Continuity Management*** **white paper**.

Article	Requirement	Referenced SAS Documents	SAS Comments
30.3.d DORA	The contractual arrangements on the use of ICT services supporting critical or important functions shall include the **obligation of the ICT third-party service provider to participate and fully cooperate in the financial entity's TLPT as referred to in Articles 26 and 27**.	• Art. 7.5 Addendum for Regulated Customers.	In order to ensure the highest quality of cloud services, SAS regularly performs independent penetration tests and may – to the extent this does not jeopardize the security of its networks – make their results available to Customers on a confidential basis. If, despite these tests and their results, a SAS Customer still needs SAS to participate in a TLPT organized by the Customer, SAS will agree the terms of such participation in accordance with the DORA requirements. For more information, please refer to the SAS white paper *EU DORA Advisory*, available on the SAS Trust Center at **https://www.sas.com/en_us/trust-center/sas-trust-compliance.html**.

Article	Requirement	Referenced SAS Documents	SAS Comments
30.3.e DORA	The contractual arrangements on the use of ICT services supporting critical or important functions shall include **the right to monitor, on an ongoing basis, the ICT third-party service provider's performance**, which entails the following: **i. Unrestricted rights of access, inspection and audit** by the financial entity, or an appointed third party, and by the competent authority, and the right to **take copies of relevant documentation on-site** if they are critical to the operations of the ICT third-party service provider, the effective exercise of which is not impeded or limited by other contractual arrangements or implementation policies. ii. The right to agree **on alternative assurance levels if other clients' rights are affected**. iii. The obligation of the ICT third-party service provider to **fully cooperate during the on-site inspections and audits** performed by the competent authorities, the Lead Overseer, financial entity or an appointed third party. iv. The obligation to provide **details on the scope, procedures to be followed and frequency of such inspections and audits**.	• Art. 7.4 Addendum for Regulated Customers.	The provisions of Art. 7.4 of the Addendum for Regulated Customers ensure that the Customer, as well as its competent supervision authority, has audit and inspection rights that meet the market standard and allow the Customer to satisfy the DORA requirements and the expectations of financial sector regulators. For information and physical safety reasons, as well as operational reasons, SAS cannot allow its Customers to execute their audit and access rights at will and without clearly set rules and procedures. The contractual solution proposed in the Addendum for Regulated Customers allows financial entities and their competent authorities to gather all the information they need to assess SAS' credibility and performance in an organized and safe manner.

Article	Requirement	Referenced SAS Documents	SAS Comments
30.3.f DORA	The contractual arrangements on the use of ICT services supporting critical or important functions shall include **exit strategies, in particular the establishment of a mandatory adequate transition period:** i. During which the ICT third-party service provider will continue providing the respective functions, or ICT services, with a view to reducing the risk of disruption at the financial entity or to ensure its effective resolution and restructuring; ii. Allowing the financial entity to migrate to another ICT third-party service provider or change to in-house solutions consistent with the complexity of the service provided.	• Art. 9 Addendum for Regulated Customers.	Art. 9 of the Addendum for Regulated Customers establishes rules of cooperation between SAS and its Customers in the event that the provision of services is terminated. The purpose of these provisions is to allow the Customer to make a smooth transition to solutions available in-house or from other providers.



For more information, please visit sas.com.