EUROPEAN COMPLIANCE SUITE

EU AI Act Compliance Evidence Templates

EXPLANATORY NOTICE AND TEMPLATE

Criticality self-assessment — an ICT third-party service provider's assessment of its position against the Article 31 designation criteria under the Digital Operational Resilience Act (Regulation (EU) 2022/2554)

Template reference	ECS-DORA-SCOPE
Version	1.0
Edition	July 2026
Regulation	Regulation (EU) 2022/2554 (DORA), Article 31 (designation of critical ICT third-party service providers)
Instrument addressed	Self-assessment against the Article 31(2) designation criteria, the Article 31(8) carve-outs, and the Article 31(12) third-country subsidiary requirement
Intended user	Technology companies (ICT third-party service providers) supplying ICT services to EU financial entities
Position in the pack	Entry document. Complete first; it establishes your exposure and what the rest of the pack must cover
Associated templates	ECS-DORA-REGISTER — Register of Information data pack; ECS-DORA-CONTRACT — Articles 28–30 checklist; ECS-DORA-SUBCONTRACT — subcontracting disclosure; ECS-DORA-INCIDENT — incident notification; ECS-DORA-TLPT — threat-led penetration testing

This explanatory notice and the accompanying template are published by European Compliance Suite as private compliance documentation. They are not an official document, are not approved by the European Supervisory Authorities, any Lead Overseer or any competent authority, and do not constitute legal advice. Designation as critical is a determination made by the ESAs, not a self-assessment; this document helps a provider understand and prepare for its position and does not itself determine designation. Legal review against the current text of Regulation (EU) 2022/2554 and its delegated and implementing acts is required before any reliance.

1. Purpose and context

(1) The Digital Operational Resilience Act (Regulation (EU) 2022/2554, "DORA") has applied since 17 January 2025, and it reaches technology companies that never considered themselves financial-sector businesses. DORA regulates the financial entities — banks, insurers, investment firms and the rest — but it does so in part by regulating their relationships with the ICT third-party service providers that supply them. If you sell ICT services to an EU financial entity, DORA reaches you through your customer: your customer must carry you in its Register of Information in a prescribed format, your contract with it must contain the terms DORA requires, and — if you are large and systemically important enough — you may be designated as a critical ICT third-party provider and brought under direct EU oversight. This document is a self-assessment of where a provider stands against that framework.

(2) Most suppliers discover all of this when a customer's procurement team sends a DORA questionnaire and a contract addendum. By then the supplier is reacting, under time pressure, to a document written from the financial entity's side. This pack exists to let a provider get ahead of that moment — to understand its own position, prepare the information its customers will need, and know which of DORA's obligations bite on it and which do not. This self-assessment is the entry point: it establishes whether the provider is likely to face designation as critical, what the ordinary (non-critical) obligations require of it, and therefore what the rest of the pack must cover.

(3) A crucial point of accuracy runs through this document. Designation as a critical ICT third-party provider is a determination made by the European Supervisory Authorities under Article 31, not something a provider declares about itself. The great majority of ICT providers to financial entities are not critical and will never be designated — as of the first official list published in November 2025, only nineteen providers were designated, all major cloud and core-platform businesses. This self-assessment does not designate anyone; it helps a provider understand how the Article 31 criteria apply to it, whether it is realistically in or out of scope for designation, and what follows either way. For most providers the valuable output is a documented, defensible conclusion that they are not critical, together with a clear view of the ordinary contractual and register obligations that do apply.

RELEVANT LEGAL TEXT

Article 31(1)–(2) DORA — Designation (abridged).

The ESAs shall designate the ICT third-party service providers that are critical for financial entities, following an assessment that takes into account the criteria in paragraph 2. The designation shall be based on all of the following criteria in relation to the ICT services provided: (a) the systemic impact on the stability, continuity or quality of the provision of financial services in the event of a large-scale operational failure of the provider; (b) the systemic character or importance of the financial entities that rely on the provider, assessed by reference to the number of global or other systemically important institutions relying on it; (c) the reliance of financial entities on the services of the provider in relation to critical or important functions that ultimately involve the provider; and (d) the degree of substitutability of the provider.

Article 31(8) — Carve-outs (abridged).

The designation shall not apply to: financial entities providing ICT services to other financial entities; ICT third-party service providers subject to certain oversight frameworks; ICT intra-group service providers; and providers offering ICT services solely in one Member State to financial entities active only in that Member State.

Article 31(12)–(13) — Third-country subsidiary.

Financial entities shall only make use of the services of an ICT third-party service provider established in a third country and designated as critical if that provider has established a subsidiary in the Union within the 12 months following designation. The critical provider shall notify the Lead Overseer of any changes to the management structure of the Union subsidiary.

2. How to use this self-assessment

(4) The self-assessment proceeds through five findings, completed in order. Each calls for reasoning rather than a bare answer, because the value — to the provider and to a customer who asks — is in the documented basis, not the conclusion alone.

- Finding A — Are you an ICT third-party service provider supplying an EU financial entity, and is DORA therefore relevant to you at all?
- Finding B — Do any of the Article 31(8) carve-outs remove you from the designation framework?
- Finding C — How do the four Article 31(2) criteria apply to you, and is designation as critical a realistic prospect?
- Finding D — If you are a third-country provider, what would the Article 31(12) twelve-month EU-subsidiary requirement mean for you?
- Finding E — What do your ordinary (non-critical) DORA-driven obligations require, and which pack documents follow?

3. The five findings

3.1. Finding A — are you in DORA's supplier scope?

(5) DORA reaches a provider through its financial-entity customers. The threshold question is whether the provider supplies ICT services — broadly defined, covering digital and data services provided through ICT systems on an ongoing basis — to one or more financial entities established in the EU. If it does, the provider's customers have DORA obligations that flow onto the provider through the contract and the Register of Information, whether or not the provider is ever designated as critical. If a provider supplies no EU financial entities, DORA does not reach it through this route. The self-assessment records the customer base and the services supplied, because that is the foundation of everything else.

3.2. Finding B — the carve-outs

(6) Before assessing the designation criteria, the provider checks the Article 31(8) carve-outs, because they remove certain providers from the designation framework entirely. The designation does not apply to financial entities that themselves provide ICT services to other financial entities; to certain providers already subject to specified oversight frameworks; to ICT intra-group service providers; and — importantly for smaller and nationally-focused providers — to providers offering ICT services solely in one Member State to financial entities active only in that Member State. A provider within a carve-out cannot be designated critical, though it still has the ordinary contractual and register obligations. The carve-out relied on, if any, is recorded with its basis.

3.3. Finding C — the four designation criteria

(7) The heart of the assessment is the four Article 31(2) criteria, which the ESAs apply together, not individually: the systemic impact of a large-scale failure of the provider on the provision of financial services; the systemic importance of the financial entities that rely on the provider (measured by how many systemically important institutions depend on it); the reliance of financial entities on the provider for critical or important functions; and the degree of substitutability of the provider. Substitutability carries the most practical weight — a provider that is easily replaced is unlikely to be designated however large, while a provider on which many significant institutions depend for a function they cannot readily move elsewhere is a candidate. The provider assesses each criterion honestly against its real customer base and market position, and reaches a reasoned conclusion about whether designation is a realistic prospect. For most providers the conclusion is that it is not, and a documented version of that conclusion is a valuable thing to be able to hand a customer.

3.4. Finding D — third-country providers and the subsidiary requirement

(8) Article 31 applies to providers regardless of where they are established: a US or Asian technology company supplying EU financial entities is assessed on exactly the same criteria as an EU provider. For a third-country provider, Article 31(12) adds a consequence that is easy to miss and expensive to meet late: if designated as critical, the provider must establish a subsidiary in the Union within twelve months of designation, or its financial-entity customers may not continue to use it. A third-country provider that is a realistic designation candidate should understand this well before any designation, because standing up an EU subsidiary is not a twelve-month afterthought. The self-assessment records the provider's establishment and, where relevant, its position on the subsidiary requirement.

3.5. Finding E — ordinary obligations and the rest of the pack

(9) Designation is the exception; the ordinary obligations are the rule and reach almost every provider to EU financial entities. Whether or not it is ever critical, a provider will be carried in its customers' Registers of Information (ECS-DORA-REGISTER), will need its contracts to contain the Articles 28–30 terms (ECS-DORA-CONTRACT), will need to disclose its subcontracting (ECS-DORA-SUBCONTRACT), will need an incident-notification process aligned to its customers' reporting clocks (ECS-DORA-INCIDENT), and — where it supports critical or important functions — may be drawn into threat-led penetration testing (ECS-DORA-TLPT). The self-assessment closes by identifying which of these apply and with what priority.

4. What designation would mean

(10) For the minority of providers for whom designation is realistic, it is worth understanding what it brings, because it changes the relationship materially. A designated critical provider is assigned a Lead Overseer from among the ESAs and comes under direct EU oversight: the Lead Overseer can request information, conduct investigations including personnel interviews, and carry out on-site inspections at the provider's premises and at its material subcontractors. The provider must notify its financial-entity customers of its designation. And, for a third-country provider, the twelve-month subsidiary requirement applies. None of this follows from a self-assessment — it follows from an ESA designation — but a provider that may be a candidate should prepare for it rather than be surprised by it.

5. Review

(11) The self-assessment is renewed when the provider's customer base or market position changes materially, when its establishment or corporate structure changes, when the ESAs update the list of designated critical providers or the delegated criteria change, and in any event at intervals not exceeding twelve months. A provider's substitutability and systemic importance are not static, and a conclusion that was sound a year ago may not hold after a period of growth.

Annex

Criticality self-assessment — provider worksheet

Assessment version	*Version identifier, with references to earlier versions where applicable.*
Date of assessment	*DD.MM.YYYY*
Completed by	*Name, function and role of the person responsible for the accuracy of this assessment.*
Provider	*Legal name, establishment (including whether EU or third-country) and LEI where held.*
Law verified on	*Date the provisions were checked against the current text of DORA and its delegated/implementing acts.*

1. Finding A — supplier scope

EU financial-entity customers	*Whether the provider supplies ICT services to one or more EU financial entities, and broadly which.*
ICT services supplied	*The ICT services provided, described in terms that will map to the service-type list in the Register data pack.*
Conclusion	*DORA reaches the provider through its financial-entity customers / does not — with the basis.*

2. Finding B — carve-outs (Article 31(8))

A carve-out removes designation but not the ordinary contractual/register obligations.

Carve-out	Applies?	Basis
Financial entity providing ICT services to other FEs		
Provider subject to a specified oversight framework		
ICT intra-group service provider		
Services solely in one Member State to FEs active only there		

Conclusion	*A carve-out applies (designation not possible) / no carve-out applies — with the basis.*

3. Finding C — designation criteria (Article 31(2))

The ESAs apply all four together. Assess honestly against real customer base and market position. Substitutability carries the most weight.

Criterion	How it applies to us	Exposure (low/med/high)
(a) Systemic impact of a large-scale failure		
(b) Systemic importance of dependent financial entities		
(c) Reliance for critical or important functions		
(d) Degree of substitutability		

Designation prospect	*Realistic / unlikely / not possible (carve-out), with reasoning. For most providers this is a documented "unlikely".*

4. Finding D — third-country subsidiary (Article 31(12))

Third-country provider?	*Whether the provider is established outside the EU.*
Subsidiary position	*If a realistic designation candidate: the provider's position on establishing an EU subsidiary within 12 months of any designation.*
EU coordination point	*Any EU entity that could act as the coordination point with the ESAs.*

5. Finding E — ordinary obligations and documents

Register of Information	*Confirmation the provider will be carried in customers' registers. Reference ECS-DORA-REGISTER.*
Contractual terms	*Whether contracts contain the Articles 28–30 terms. Reference ECS-DORA-CONTRACT.*
Subcontracting	*Whether the provider subcontracts any part of the service. Reference ECS-DORA-SUBCONTRACT.*
Incident notification	*Whether an incident-notification process aligned to customers' clocks exists. Reference ECS-DORA-INCIDENT.*
TLPT	*Whether the provider supports critical or important functions and may be drawn into threat-led penetration testing. Reference ECS-DORA-TLPT.*
Priorities and owners	*Which obligations are most pressing, who owns each, and by when.*

6. Review

Next scheduled review	*DD.MM.YYYY, no later than twelve months after the date of assessment.*
Trigger events	*Material growth, structural change, ESA list or criteria change.*

7. Version history and declaration

Version	Date	Nature of change or review	Approved by

Declaration

This self-assessment is made in good faith and, to the knowledge of the signatory, is accurate and complete as at the date of signature. It does not constitute or substitute for a designation determination by the European Supervisory Authorities.

Name	
Function	
Date	
Signature	