CHECKLIST · DORA AND THE IDENTITY PROVIDER

Is the identity provider in your DORA programme? A checklist.

Every single sign-on application depends on the identity provider, so it is an ICT service that supports critical or important functions. The Digital Operational Resilience Act, Regulation (EU) 2022/2554, has applied to EU financial entities since 17 January 2025. This checklist lists the questions a supervisor or auditor can ask about the identity provider, by DORA article, and the evidence that answers each one.

Art. 8 Identification and inventory

Check	Evidence that answers it
☐ The identity provider is recorded as an ICT asset that supports critical or important functions.	Asset register entry with its owner.
☐ Every application that signs in through it is listed with its protocol, owner and the business function it supports.	Dated application inventory.
☐ The dependencies are mapped: which functions stop when the identity provider is unavailable, and which applications have another way in.	Dependency map.
☐ Signing certificates and client secrets are listed with their expiry dates.	Credential inventory with expiry.

Art. 9 Access control and strong authentication

Check	Evidence that answers it
☐ Every administrative role in the identity provider has a named holder and a recorded reason.	Privileged access review, signed off.
☐ Administrators sign in with strong authentication, phishing-resistant where the provider supports it.	Sign-in policy for administrator roles.
☐ Permissions granted to integrations and API clients are limited to what each one needs.	Review of application permissions.
☐ Emergency access accounts exist, are kept out of the normal sign-in policy on purpose, and are tested.	Test record of the emergency accounts.

Art. 11, 12 Backup, restoration and continuity

Check	Evidence that answers it
☐ The configuration of every application integration is backed up, not only users and groups.	Backup log with the applications it covers.
☐ A restoration from that backup has been tested and the result documented.	Restoration test report.
☐ Restoration does not depend on the failed system: Article 12 asks that restoring on your own systems uses systems segregated from the source.	A standby tenant, or a tenant at another provider.
☐ Recovery time and recovery point targets are set for the functions that depend on the identity provider.	Business impact analysis.
☐ The continuity and response plans cover the identity provider being unavailable or compromised, and are tested at least yearly.	Plan and the last test record.

Art. 24, 25 Resilience testing

Check	Evidence that answers it
☐ The testing programme includes a scenario where the identity provider is unavailable and one where it is compromised.	Testing programme and scenarios.
☐ A failover has been rehearsed for a pilot group and timed against the recovery target.	Execution log of the rehearsal.
☐ Findings from the tests are tracked until they are closed.	Findings register.

Art. 28, 30 Third-party risk and exit

Check	Evidence that answers it
☐ The identity provider contract is in the register of information.	Register of information entry.
☐ An exit strategy names an alternative provider and a transition plan for the identity provider.	Exit plan, reviewed and tested.
☐ The contract has an adequate transition period, and the exit plan's schedule fits inside it.	Contract clause and exit timeline.
☐ The time to move every application to the alternative provider is measured from the inventory, not estimated.	Migration plan with a per-application count.

Art. 17–19 Incident management and reporting

Check	Evidence that answers it
☐ The incident process covers an outage or a compromise of the identity provider, with classification criteria.	Incident procedure and classification table.
☐ The provider's own status is monitored, so an outage is detected from its report as well as from user tickets.	Status monitoring, for example idp-status.tenantflex.com.
☐ Configuration changes in the identity provider are recorded, so an investigation can show what changed and when.	Change history or daily configuration diffs.

TenantFlex

How TenantFlex produces the evidence

Feature	Articles	What it gives you
Discovery	8	Read-only inventory of every SAML and OIDC application, its claims, assignments, certificates and secrets with expiry.
Privileged access review	9	Administrative roles and application permissions in each tenant, for a reviewed and signed-off list.
Backup and restore	12	Scheduled captures of every application, compared with the last one, with a restore of the fields that changed.
Standby tenant	11, 12, 28	The critical applications staged at another provider and kept current, which is the alternative an exit plan names.
Rehearsed cutover	24, 25, 28	A failover run as a migration job for a pilot group, with an execution log and a measured duration.
Identity provider status	17–19	A public page that reads the public status reports of Entra ID, Okta and PingOne.

This checklist is a starting point for a discussion with your risk, audit and legal teams. It is not legal advice. References are to articles of Regulation (EU) 2022/2554 (OJ L 333, 27.12.2022); check the paragraphs, the regulatory technical standards and the guidance of your competent authority before relying on them.

Start with the inventory.

A read-only discovery run answers the Article 8 questions and gives the application count an exit plan needs. Ask for one at info@tenantflex.com.