Is your organisation ready for AMLR, eIDAS 2.0 and SCA in 2027?

Published by Authologic | Regulatory status current as of 19 October 2026 | This document is a self-assessment tool, not legal advice.

Key sources: Regulation (EU) 2024/1624 (AMLR) | Regulation (EU) 2024/1183 (eIDAS 2.0) | PSD2 (Directive (EU) 2015/2366) and the RTS on SCA | AMLA consultation on draft CDD RTS (Feb-May 2026) | AMLA final draft CDD RTS submitted to the European Commission (1 October 2026) | Authologic analysis: "How eIDAS 2.0 affects private relying parties and SCA" (March 2026) | Regulatory positions reflect the state of play on 19 October 2026 and may change as implementing acts are adopted.

How to use this checklist

Two EU regulations reshape identity verification in 2027. **The Anti-Money Laundering Regulation** (AMLR, Regulation (EU) 2024/1624) applies from July 10, 2027. The obligation for private relying parties to accept the **EUDI Wallet** under **eIDAS 2.0** follows on December 24, 2027, with **Strong Customer Authentication** (SCA) remaining governed by **PSD2** until the **Payment Services Regulation** (PSR) applies - not before the second half of 2028.

This checklist turns both regimes into a **practical self-assessment**. It is written for a **high-level analysis by compliance officers and product owners**. No legal background required. Work through each question and tick **Yes**, **In progress**, or **No** in the table. Answer honestly - the goal is to find gaps while there is still time to close them. Section 7 tells you how to read your score.

Section 1 | Scope: do these rules apply to you?

Question	Yes	In progress	No
1.1 Taking into account relevant sectoral regulations, have you determined whether your organisation falls within the scope of Art. 5f(2) of eIDAS 2.0 (banking, financial services, telecom, health, education, energy, transport, and others)? *Why this matters: Under Art. 5f(2), accepting the EUDI Wallet becomes mandatory wherever strong user authentication for online identification is required by law or contract. Micro and small enterprises are exempt. If you are in scope, wallet acceptance is not optional after December 24, 2027.*	☐	☐	☐
1.2 Have you assessed whether your organisation qualifies as a "private relying party" - a natural or legal person relying on electronic identification or trust services? *Why this matters: Relying party status is the trigger for most eIDAS 2.0 obligations, including registration in a dedicated register and identity wallet acceptance. Many companies hold this status without realising it, for example through login or e-signature flows.*	☐	☐	☐
1.3 Do you know in which Member State(s) you must register as a relying party, and have you defined the purpose and data scope for that registration? *Why this matters: Registration happens in your Member State of establishment and must state why you use the identity wallet and which data you request. Getting the data scope wrong means re-registration or non-compliant data requests later.*	☐	☐	☐
1.4 Have you confirmed whether your organisation is an "obliged entity" under AMLR - including newly in-scope categories such as crypto-asset service providers, crowdfunding platforms and traders in high-value goods? *Why this matters: AMLR widens the obliged-entity list compared with the AML directives. Organisations entering scope for the first time should consider building a compliance framework from scratch before July 2027, not adapt an existing one.*	☐	☐	☐
1.5 If you operate in multiple EU markets, have you mapped which national requirements survive alongside the harmonised rulebook? *Why this matters: AMLR removes most national variation, but Member States keep some local rules and AMLD6 still requires national transposition. A single-rulebook assumption without a country check leaves blind spots.*	☐	☐	☐

Section 2 | Timeline: where are you against the deadlines?

Question	Yes	In progress	No
2.1 Does your compliance roadmap account for December 24, 2026 - the date each Member State must provide at least one EUDI Wallet? *Why this matters: This is the formal availability deadline; in practice several Member States are expected to go live in early 2027. Every wallet launched from this date is a wallet your users may present to you 12 months later.*	☐	☐	☐
2.2 Does it account for December 24, 2027 - the date private relying parties (except micro and small enterprises) must accept the EUDI Wallet wherever strong user authentication for online identification is required by law or contract? *Why this matters: This is the hard compliance deadline for wallet acceptance. Architecture, integration and registration must be complete before this date, because readiness depends on technical implementation, not policy declarations.*	☐	☐	☐
2.3 Does it account for July 10, 2027 - the date AMLR applies directly across all Member States? *Why this matters: AMLR needs no national transposition. It applies as written, five months before the wallet acceptance deadline, and supervisors will expect compliant CDD from day one.*	☐	☐	☐
2.4 Are you tracking wallets and eID schemes launching ahead of the deadlines? *Why this matters: Adoption has already started - Denmark's AltID is live, and more will follow around the deadline. Waiting for the legal deadline means arriving after your users and competitors.*	☐	☐	☐
2.5 Have you allocated budget and engineering capacity for identity infrastructure changes in 2026, not 2027? *Why this matters: Both regimes converge on the same infrastructure in the same year. Teams that plan integration work for 2027 will compete for resources against every other regulated business doing the same.*	☐	☐	☐

Section 3 | SCA architecture readiness (PSD2, PSR and eIDAS 2.0)

Question	Yes	In progress	No
3.1 Have you mapped which of your authentication flows will fall under PSR instead of PSD2? *Why this matters: After PSR becomes applicable, SCA will be governed mainly by the directly applicable PSR, not by PSD2 anymore. Flows designed for PSD2 assumptions need review, not automatic carry-over.*	☐	☐	☐
3.2 Can your architecture support wallet-based SCA in remote scenarios, such as account access and electronic payment initiation? *Why this matters: Consumers gain the right to perform SCA with the EUDI Wallet in remote flows. Your systems must accept it wherever strong user authentication for online identification is required by law or contract, even if most users keep existing methods.*	☐	☐	☐
3.3 Does your SCA design support mandatory dynamic linking under PSD2 and the RTS on SCA (later under the PSR)? *Why this matters: Dynamic linking ties each authentication to a specific amount and payee. Aligning wallet-based authentication with this requirement is one of the hardest parts of the implementation phase.*	☐	☐	☐
3.4 Can you meet the requirements of PSD2 and the RTS on SCA (later the PSR) for secure credential storage? *Why this matters: The RTS on SCA (and later the PSR) require credentials to be stored and handled securely across the whole authentication chain. Wallet integration adds new components to that chain, and each one must meet the bar.*	☐	☐	☐
3.5 Can you support cross-application authentication flows in mobile environments - from wallet app to your app and back? *Why this matters: Wallet-based SCA on a phone means the user leaves your app, authenticates in the wallet, and returns. Broken hand-offs kill conversion and create security gaps.*	☐	☐	☐
3.6 Have you confirmed which flows are out of scope, such as in-person point-of-sale and ATM transactions? *Why this matters: The wallet acceptance obligation is framed around remote scenarios; in-person POS and ATM are generally read as out of scope, though parts of the market are preparing proximity support. Knowing what is out of scope stops you from over-engineering and lets you focus on the budget where the mandate actually bites.*	☐	☐	☐
3.7 Will users be able to choose between the wallet and your existing SCA methods, with the wallet option available wherever strong user authentication for online identification is required by law or contract? *Why this matters: Users stay free to choose their method. Your obligation is availability: the wallet path must exist and work, in parallel with what you run today.*	☐	☐	☐

Section 4 | Wallet acceptance readiness

Question	Yes	In progress	No
4.1 Do you have a strategy for acceptance and interoperability testing of a minimum of 27 national EUDI Wallets? *Why this matters: Each Member State ships at least one wallet, and both governments and accredited private entities can issue them. One integration is a pilot; 27+ is an orchestration problem.*	☐	☐	☐
4.2 Can your systems verify the authenticity and validity of a presented wallet using the common protocols and interfaces? *Why this matters: eIDAS 2.0 standardises how wallets present data and how relying parties verify it. Building against the common protocols once beats reverse-engineering each wallet separately.*	☐	☐	☐
4.3 Can you authenticate yourself to the wallet as a registered relying party? *Why this matters: Wallets verify you before releasing data. Relying party authentication is a two-way mechanism, and your registration credentials are part of the technical flow, not just paperwork.*	☐	☐	☐
4.4 Are your data requests limited to what is necessary and proportionate, including support for selective disclosure? *Why this matters: Data minimisation is a legal requirement, not a design preference. Requesting more attributes than your registered purpose allows is a compliance failure even if the user consents.*	☐	☐	☐
4.5 Do you have a plan for wallet acceptance beyond your home market? *Why this matters: Wallets work cross-border under common standards. A user from any Member State can present their national wallet to you, so single-market readiness is not readiness.*	☐	☐	☐
4.6 Have you decided between building integrations in-house and using an orchestration layer, and modelled the maintenance cost of each? *Why this matters: The build-vs-orchestrate decision compounds over time: every new wallet, version change and certification update lands on whoever owns the integrations. Model the five-year cost, not the first integration.*	☐	☐	☐

For a deeper wallet-specific assessment, see: EUDI Wallet Readiness Checklist by Authologic.

Section 5 | AMLR / CDD readiness

Question	Yes	In progress	No
5.1 Have you mapped your current KYC flows against AMLR Article 22 - verification of name, date of birth, nationality and address against reliable, independent sources? *Why this matters: Article 22 defines the CDD data points and requires verification against authoritative sources, not self-declaration. Legacy flows built on document collection alone will need remediation before July 2027.*	☐	☐	☐
5.2 Can your onboarding support the verification pathways AMLR recognises: identity documents together with information from reliable and independent sources, or electronic identification means at substantial or high assurance together with relevant qualified trust services - the EUDI Wallet being one such means? *Why this matters: Article 22(6) names these digital pathways alongside document-based remote onboarding. Supporting them is how CDD and eIDAS 2.0 investment converge into one infrastructure instead of two parallel projects.*	☐	☐	☐
5.3 Are you tracking the Customer Due Diligence Regulatory Technical Standards - AMLA's final draft, sent to the European Commission on October 1, 2026, and the date they will apply, six months after entry into force? *Why this matters: The CDD RTS set the binding technical benchmark supervisors will assess you against. AMLA sent its final draft to the European Commission on October 1, 2026; once adopted, the standards apply six months after entry into force, so the implementation window is short.*	☐	☐	☐
5.4 Do your CDD thresholds match AMLR - EUR 10,000 for occasional transactions, EUR 3,000 and above for occasional cash transactions, and limited CDD below EUR 1,000 for crypto-asset transfers? *Why this matters: The occasional-transaction threshold drops from EUR 15,000 to EUR 10,000. Thresholds hard-coded into onboarding logic and monitoring rules must change before the regulation applies.*	☐	☐	☐
5.5 Are your enhanced due diligence triggers aligned with AMLR - PEPs, high-risk third countries, business relationships involving assets of EUR 5 million or more, and customers with net worth above EUR 50 million? *Why this matters: AMLR names specific EDD triggers, but EDD also applies to any other higher-risk case you identify yourself. Your risk engine must recognise both and apply deeper checks with evidence.*	☐	☐	☐
5.6 Are you prepared for supervision under AMLA, including the five-working-day deadline for responding to Financial Intelligence Unit requests? *Why this matters: AMLA has been operational since July 2025 and starts direct supervision of selected institutions in 2028. The five-day FIU deadline is a strict legal requirement that assumes your customer data is retrievable on demand.*	☐	☐	☐

Section 6 | Evidence, monitoring and audit trail

Question	Yes	In progress	No
6.1 Can your systems maintain CDD data as a living record, with defined refresh triggers and re-verification logic? *Why this matters: CDD stops being collect-once-and-file. AMLR expects data-age rules and defined triggers for re-verification, so customer records must update as circumstances change.*	☐	☐	☐
6.2 Does your ongoing monitoring cover the whole business relationship - transaction monitoring plus regular and event-driven updates of customer data - rather than relying on periodic sample checks? *Why this matters: Article 26 of the AMLR sets hard maximum intervals for updating customer information (1 year for higher-risk customers, 5 years for others) on top of event-driven reviews, and requires transaction monitoring that can detect unusual or suspicious activity - also under simplified due diligence. Automation is not mandatory, but sample checks alone are unlikely to be enough.*	☐	☐	☐
6.3 Can you produce an audit trail showing which verification method, at which assurance level, was used for which customer? *Why this matters: Supervisors will ask not just whether you verified a customer, but how and at what assurance level. Method-level evidence is what separates a defensible CDD file from a finding.*	☐	☐	☐

Section 7 | Scoring and next steps

Count your answers across all 32 questions.

Result	What it means	What to do next
Mostly YES	You are ahead of the market.	Close the gaps marked In progress. Pressure-test wallet integrations against the RTS and implementing acts as they are finalised.
MIXED	You have started, but 2027 readiness is not secured.	Prioritise Sections 3 and 5 - SCA architecture and CDD remediation have the longest lead times. Set milestones for Q4 2026.
Mostly NO	This is a 2026 priority, not a 2027 one.	Confirm scope first (Section 1), then build a roadmap backwards from July 10, 2027 - the earlier hard deadline.

A note on the integration problem:
Most of this checklist reduces to one capability: accepting many identity methods, at defined assurance levels, with evidence. That is an orchestration problem, not a series of one-off integrations. Platforms like **Authologic** exist for exactly this reason: national eIDs, government identity wallets, biometrics and document-based verification in a single API (100+ identity methods across 230+ countries and territories).

Build or buy, the architectural question is the same:
Can you add the next wallet, eID scheme or attestation type without rebuilding your stack?

Verifying every user with the best method available, at the lowest cost and with the least friction. | Book a meeting

What to Do Next

July 2027 will not wait for procurement cycles.



Turn your score into a plan

We work with banks and other regulated businesses across Europe to map identity infrastructure gaps - from wallet acceptance to AMLR-ready verification - without rebuilding your stack from scratch.



Find out more about how Authologic works

Check how our identity orchestration platform connects EUDI Wallets, national eIDs, bank-based verification, and document checks through a single API - one integration serving both SCA and CDD requirements.

Version 3 - updated 19 October 2026