Article 12 logging review checklist

A structured discussion aid. Statutory logging questions and optional integrity mechanisms are separated. This is not a compliance assessment, legal opinion or certification.

1. Determine the applicable system and role

[ ] Identify the system, intended purpose, territory, provider/deployer role and accountable owner.

[ ] Ask qualified counsel to determine whether the system is high-risk under the applicable classification rules, including exceptions and transitional treatment. Do not classify all finance, fraud, AML/KYC or insurance systems together.

Annex III 5(b) includes natural-person creditworthiness/credit scoring but expressly excludes systems used to detect financial fraud from that category. This does not determine classification under other provisions.

[ ] Check the current application date and any rules for systems already on the market. The Commission currently lists 2 December 2027 for Annex III high-risk rules and 2 August 2028 for regulated-product high-risk rules. Other obligations can apply independently.

2. Article 12 logging capability questions

[ ] Can the high-risk system technically allow automatic recording of events over its lifetime?

[ ] Is traceability appropriate to its intended purpose, including recording events relevant to identifying risks or substantial modification, post-market monitoring and system operation?

[ ] If the remote biometric identification provisions apply, do the logs cover the specified periods of use, reference database, matching input and people verifying results?

Article 12 does not prescribe SHA-256, hash chains, RFC 3161 timestamps, a third-party verifier, or a universal input/output/model/policy record format for every AI decision.

3. Retention and access are separate questions

[ ] Identify which records are under the provider or deployer's control, how long they must be retained, the applicable legal basis and any constraints on personal data.

Article 19 addresses providers' automatically generated logs, including an appropriate period of at least six months unless applicable law provides otherwise. Financial-sector documentation rules and deployer obligations need their own assessment. This is not an unconditional retention rule derived from Article 12 alone.

[ ] Agree who may access, export or delete records, secure transfer arrangements, retention ownership, incident contacts and the handling of customer information.

4. Optional technical integrity checks

The following are implementation options to assess against the review question and risk. They are not presented as Article 12 requirements.

[ ] Recompute record hashes from the declared canonical representation and profile.

[ ] Check chain links and export boundaries against independently retained references where available.

[ ] If a timestamp token is used, verify its signature and root binding against a certificate obtained independently from the intended authority.

[ ] Show that an altered record fails the expected check. Assess missing-event detection separately through source reconciliation.

A valid timestamp supports that an anchored root existed no later than the token time. It does not prove the exact time of every event. A consistent chain does not prove complete capture, source accuracy, authorised approval, actual enforcement or a correct decision.

5. Start with a bounded reconstruction

[ ] Select one historical action and ask what the request, controls, approval authority, execution receipt and outcome records establish.

[ ] Separate supported findings, missing artifacts and conclusions that remain unknown. Assign an owner to each follow-up.

Review the US$2,500 assessment scope and the synthetic Evidence Readiness Record. Do not send sensitive records before handling is agreed.

Primary sources, checked 21 October 2026

Article 12

Article 19

Annex III

Commission implementation timeline