

MaxAudit AuditEngine – Process Flow & Deviation Matrix

Version: 1.0

Issued by: SAC, Take Back Your Data (TBYD)

License: MaxOneOpen License v2.2 – Structurally Enforced

1. Function of the AuditEngine

The AuditEngine serves as the central execution logic within the MaxAudit framework. It coordinates all verification steps, manages error paths, and ensures deterministic interpretation of architectural deviations. It operates identically in both the Dongle and Verifier modules.

2. Process Flow

The verification process follows a modular, stateless execution model. The flow is strictly deterministic and reproducible:

1. Load signed reference schema (CryptoKernel)
2. Extract live system structure via interface adapters
3. Normalize system input and validate against reference
4. Identify and classify architectural deviations
5. Encode audit result (OutputEncoder)
6. Generate signed audit protocol

3. Deviation Classification Matrix

Severity	Description	Effect on Audit Status
Level 0 – None	No deviation found.	Green – Fully compliant
Level 1 – Minor	Non-critical variation (e.g., log structure mismatch).	Yellow – Remediation advised
Level 2 – Structural	Missing or altered MaxInstance modules.	Yellow – Remediation mandatory
Level 3 – Critical	Violation of license constraints or audit core logic.	Red – Immediate deactivation required
Level 4 – Tamper	Evidence of manipulation, bootloader compromise, or crypto mismatch.	Red – System disqualified

4. Deterministic Behavior

The AuditEngine ensures that identical inputs always yield identical results. Its evaluation logic is cryptographically anchored, stateless between runs, and does not rely on external conditions. This guarantees objectivity and reproducibility even under contested conditions.

5. Error Handling & Resilience

- All faults are logged internally within the audit trace.
- Failures do not halt the engine but are classified and reported.
- Recovery paths are predefined for each deviation level ≤ 2 .

6. Signature Logic

Every audit run concludes with a SHA-256 based signature over the evaluation graph, timestamp, and result hash. This signature is independently verifiable and cross-linked with the Fork Registry if applicable.

7. Deployment Modes

- Dongle mode: read-only, stateless, no storage retained
- Verifier mode: CI/CD integration possible, audit trace optionally retained for internal compliance