# Module 27 – Predictive Governance & AI Capsule

Version: 4.1 | Classification: Capsule-Driven Predictive Control Logic  
Scope: Integration of machine learning, predictive audit support, and zero-knowledge mechanisms into MaxOneOpen runtime governance.

**Capsule Initialization**

This capsule is instantiated when predictive control logic, anomaly simulation, or AI-supported audit interpretation is activated within a certified MaxOneOpen runtime. Its activation is mandatory whenever ML inference, capsule scoring, or automated deviation detection interacts with runtime decision vectors.

**0. Purpose & Predictive Control Premise**

This capsule provides the foundation for predictive and AI-supported runtime governance. It introduces logic constraints, structural explainability requirements, and risk isolation for machine learning components interfacing with capsule-based environments.

**1. Structural Boundaries for AI Integration**

- All ML modules must operate within non-authoritative observability capsules.

- Inference outputs may advise governance but cannot override runtime policy enforcement.

- Capsule isolation must prevent model drift, training leakage, or unauthorized retraining.

**2. Predictive Anomaly Detection Layer**

- Runtime signal analysis is used to detect execution anomalies, trust divergence, and rollback conditions.

- Capsule scoring models are trained on certified audit lineage and runtime outcomes.

- Detected anomalies trigger simulation capsules for verification without affecting active flows.

**3. Explainability & Audit Trace Logic**

- All AI decisions must be structurally explainable and snapshot-reproducible.

- Capsule logs include model version, decision vector, and observability context.

- Black-box models are prohibited in runtime-relevant decision capsules.

**4. Zero-Knowledge & Multiparty Integration**

- Capsule commitments may be validated via zero-knowledge proofs (ZKP) without exposing payloads.

- Secure multiparty execution may support capsule verification across federated jurisdictions.

- ML-triggered privacy capsule revalidation must follow runtime-bound consent lineage.

**5. Operational Constraints & Enforcement**

- No ML component may alter runtime state directly.

- Federation runtimes must certify any predictive models via auditable registration capsules.

- Deployment of AI-enhanced capsules requires signature from federation-approved model registry.

**6. Roadmap Commitments (v4.2 aligned)**

- Capsule-native explainability framework for audit AI outputs.

- Federated model registry with runtime deployment approvals.

- ML-suggested policy simulation sandbox with rollback assurance logic.

**Final CTO Statement**

This capsule defines the only permitted method to integrate predictive AI into MaxOneOpen without compromising structural integrity. It ensures explainability, enforcement isolation, and audit lineage continuity for any ML-supported process. Its use is mandatory for all federated deployments engaging with predictive runtime analysis or capsule optimization.