# Module XX – Audit Observer & Capsule Alerting Framework

Version: 4.1 | Classification: CTO Mandatory (Runtime Observation & Risk Signaling)

Scope: Live monitoring, policy violation signaling, runtime anomaly detection

## 0. Purpose & Real-Time Observation Requirement

This module defines the runtime observability, signaling interface, and trust-sensitive alert logic for MaxOneOpen v4.1. It enables system actors to detect critical execution anomalies, replay attempts, fork divergence, and policy conflicts in real time. The alert framework is capsule-based and required for audit visibility, operational response, and runtime trust escalation.

## 1. Audit Observer Roles & Event Visibility

Three observer roles are defined:  
- Sovereign Audit Node (SAN): full capsule path trace and anomaly alerts  
- Operational Observer: limited visibility on sandbox, manifest, fork, and replay flows  
- Public Observer: access to rule-level alert summaries and global trust shifts  
Observers are notified via streaming capsule feed (signed & hash-chain bound).

## 2. Capsule Alert Types & Emission Triggers

Alert Capsules include:  
- `Fork Divergence Alert Capsule (FDAC)`  
- `Replay Attempt Capsule (RAC)`  
- `Policy Collision Capsule (PCC)`  
- `Audit Chain Drift Capsule (ACDC)`  
- `Unauthorized Capsule Origin Alert (UCOA)`  
Triggers:  
- fork chain mismatch  
- repeated capsule hash in wrong time window  
- audit ledger desynchronization  
- manifest mismatch with trust declaration

## 3. Alert Overlay Channels & Capsule Trace View

Alerts are dispatched to runtime overlays:  
- Trust Zone Alert Overlay  
- Capsule Chain Divergence Map  
- Fork Trace Heatmap Viewer  
- Execution Policy Monitor  
Each alert is anchorable into the Ledger (Module 13) and replayable via Module 14.

## 4. Runtime Hook Integration & Auto-Response Logic

Alert hooks may be triggered from:  
- Manifest Engine (Module 06)  
- Ledger Commit Path (Module 13)  
- Audit Capsule Checker (Module 14)  
- Certification Validator (Module 17)  
Optional responses:  
- policy freeze  
- sandbox isolation  
- fork quarantine initiation  
- temporary certification suspension

## 5. Certification & Operational Readiness Impact

Absence of this alerting layer disqualifies deployments from real-time certified trust enforcement. Modules 17 and 18 must reference active alert coverage before reentry or certification confirmation. All emitted alerts must be signed, anchored, and publicly traceable when required.