**Compliance & Audit Logging Framework**

**Objective:**  
Implement a traceable and tamper-proof logging mechanism to ensure accountability, aid forensic analysis, and meet regulatory compliance standards.

**Detailed Components:**

* **Tracked Events:**
  + User authentication (login, logout, failed attempts).
  + Record changes (create, update, delete) with before/after state.
  + Role modifications, access control updates, data exports.
* **Log Design:**
  + **Structured logs** with timestamp, user ID, IP address, event category, outcome, and device ID.
  + UUID tracking for cross-system event correlation.
* **Storage & Retention:**
  + Logs stored in a **Write-Once-Read-Many (WORM)** format.
  + Retention policy: **7 years** minimum, with auto-archival and deletion policies.
* **Tamper Detection:**
  + Use of **hash chaining** or blockchain-based log integrity mechanisms.
  + Alerts for suspicious patterns (e.g., brute force, mass deletions).
* **Compliance Alignment:**
  + GDPR, Kenya Data Protection Act, HIPAA (if applicable).
  + Internal HR policy alignment and third-party auditor requirements.
* **Access Controls:**
  + Audit logs viewable only by compliance and super-admin roles.
  + Real-time monitoring dashboard with role-based access.