can you write same for belwo story in detail

5. Audit Store User Story: As an auditor, I want to view immutable logs of all key compliance actions and decisions for any entity, so I can satisfy internal and external regulatory reviews. Acceptance Criteria: Every critical action (screen, block, override, release, rule edit) is logged with user, timestamp, entity, and context. Logs are tamper-evident and accessible by permissioned users. One-click export of filtered or full logs for audits. Real-time monitoring dashboard available for managers

Here is a detailed, industry-standard breakdown for your Audit Store story, designed for high-assurance compliance platforms.

Audit Store – Detailed User Story

Title: Immutable, Permissioned Audit Logging and Monitoring

Description

As an auditor, I want to view, search, and export immutable logs of all important compliance actions and decisions on any business entity (orders, rules, partners, licenses), so that I can satisfy rigorous internal controls and external regulatory reviews.[1] [2] [3]

Functional Requirements (Expanded)

- **Comprehensive, Automatic Event Logging**
  - Every critical workflow action is logged: screening, block, override, release, rule edit, manual review, integration sync, and external API calls.[2] [1]
  - Each log entry includes: event type, affected entity (with unique ID/ref), user/actor (system or person), source IP, timestamp (in UTC, ISO 8601), action details, and contextual snapshot (e.g., input parameters, result, exception info).
- **Tamper-evident, Immutable Storage**
  - Logs are stored in an append-only, write-once data store (e.g., blockchain, WORM storage, or cryptographically hashed chained records) to ensure audit integrity.[4] [5] [2]
  - Any attempt to modify or delete logs triggers an alert and creates a separate, permanent error log event.
- **Access Control and Permissions**

    - Fine-grained, role-based access: only authorized users with “Audit View” permissions (e.g., auditors, compliance managers) can view sensitive logs.
    - Log access attempts (success, failure, export, or search) are themselves logged and auditable for full traceability.[1]
- **Intuitive Search, Filtering, and Export**
    - Users can easily search/filter logs by event type, entity, user, date/time, or status using intuitive forms or tags.
    - Supports partial, fuzzy, and advanced (logic) queries for multi-parametric reviews.
    - One-click export of filtered result set or full logs to PDF or CSV, with audit trail of export actions.
- **Real-Time Monitoring Dashboard**
    - Visual, real-time dashboard surfaces audit metrics: compliance alert rates, override frequencies, top actors, rule change statistics, recurring issues.
    - Drill-down capability: select a metric to see underlying logs/events.
    - Configurable, time-window summary views and exportable visualizations.
- **Compliance Alignment**
    - Log retention policies enforced per-regulation (e.g., 6+ years for HIPAA, 1–3 years for SOX, PCI DSS, ISO/SOC2).[4]
    - Chain-of-custody integrity for legal admissibility: logs digitally signed or hashed; integrity can be verified independently.
    - Supports both internal and external audit workflows—organizations can delegate temporary read access for auditors, with full tracking.

Non-Functional Requirements

- Log events must be written asynchronously and not impact application latency (target write latency: <150ms per event).[6] [7]
- The system must support storage and instant retrieval of logs scaling to millions of events across multi-year retention.
- Log queries and exports must honor access control and never leak data; encrypted at rest and in transit.
- GDPR/compliance: Support log redaction and metadata-only logs for sensitive data in strict jurisdictions.[4]

Example Scenarios

- An external regulator requests “all override actions by user X on license Y since Jan 1, 2025.” Auditor searches, reviews, exports logs, and shares the encrypted export with the regulator. All export actions are also logged.
- Compliance manager reviews daily dashboard—sees a spike in order blocks—drills into detailed logs to find it's due to a recent rule change, then links to that rule’s edit history for further forensic review.
- IT security officer is alerted to a failed attempt to tamper with log storage. The event is flagged, and forensics team accesses immutable error logs.

This approach guarantees legal-grade audit trails, maximizes compliance confidence, makes investigations efficient, and aligns with the latest industry guidance on logging, forensics, and regulatory readiness.[3] [5] [2] [1] [4]

⁂

1. https://www.digitalguardian.com/blog/audit-log-best-practices-security-compliance
2. https://log-locker.com/en/blog/guide-to-audit-logs
3. https://sjemed.com/?mno=195681
4. https://auditboard.com/blog/security-log-retention-best-practices-guide
5. https://ijsoc.goacademica.com/index.php/ijsoc/article/view/1345
6. https://www.datadoghq.com/knowledge-center/audit-logging/
7. https://www.permit.io/blog/audit-logs
8. https://simplerqms.com/21-cfr-part-11-audit-trail/
9. https://ieeexplore.ieee.org/document/11157488/
10. http://ieeexplore.ieee.org/document/6291450/
11. https://www.semanticscholar.org/paper/3a6f8de83554393b900dd4fec68eecc6c7f12982
12. https://link.springer.com/10.1007/978-3-030-29959-0_33
13. http://link.springer.com/10.1007/978-3-642-12814-1_18
14. https://www.semanticscholar.org/paper/d4adb6086e76e4baf45dcb4e91c8773a483e53a7
15. https://www.cambridge.org/core/product/identifier/S2056472424006240/type/journal_article
16. https://ecohumanism.co.uk/joe/ecohumanism/article/view/5178
17. https://elibrary.ru/item.asp?id=50254349
18. https://learn.microsoft.com/en-us/purview/audit-log-activities
19. https://ieeexplore.ieee.org/document/9643670/
20. https://www.splunk.com/en_us/blog/learn/audit-logs.html
21. https://compliancy-group.com/hipaa-audit-log-requirements/
22. https://learn.microsoft.com/en-us/purview/audit-search