

Purpose:

This runbook defines a safe, UI-only implementation for the Admin Audit Viewer.

It allows administrators and auditors to review audit events without any ability to modify data.

The UI must strictly consume existing read-only audit APIs.

Global Constraints:

- Do not modify backend audit schema or APIs
- Do not introduce write, update, or delete operations
- Do not bypass tenant isolation
- Do not expose cross-tenant data
- Do not allow filtering by arbitrary fields
- Assume Phase 6 (Audit & Observability) is complete

Capabilities Covered:

- View audit events for the current tenant
- Filter audit events safely
- Paginate results
- Inspect event details (read-only)
- Copy correlation IDs

Step 1 — Audit Viewer Page:

Route:

- /admin/audit

Behavior:

- Fetch audit events from GET /api/admin/audit-events
- Scope strictly to authenticated tenant
- Always paginate results
- Default sort: newest first

Columns to Display:

- Timestamp
- Action
- Actor email
- Actor type
- Target type / target ID
- IP address
- Correlation ID (copyable)

Step 2 — Safe Filters:

Allowed filters only:

- Action (dropdown or exact match)
- Actor (email or user ID)
- Date range (from / to)

Rules:

- No free-text search
- No JSON metadata querying
- No cross-tenant filters

Step 3 — Event Detail View:

- Expand row or side panel
- Show full event details:
 - Action
 - Actor
 - Target
 - Timestamp
 - Correlation ID
- Metadata (read-only, JSON formatted)
- No editing or deletion

Step 4 — Pagination:

- Cursor-based pagination only
- Disable infinite scrolling
- Show clear “Next / Previous” controls

Step 5 — Empty & Error States:

- Show empty state if no events
- Show generic error message on failure
- Do not expose backend errors

Audit Awareness:

- UI must never write audit events
- UI must never infer or calculate audit data
- All audit integrity guarantees are enforced server-side

Success Criteria:

- Admins can review tenant audit history safely
- Audit data is immutable and read-only
- UI does not impact performance or security
- Tenant boundaries are strictly preserved

Out of Scope:

- CSV or PDF export
- Cross-tenant audit views
- System-level audit dashboards
- Alerting or notifications
- Advanced analytics