**Phase 9: Reporting, Dashboards & Security Review — Event Management System**

**Objective**

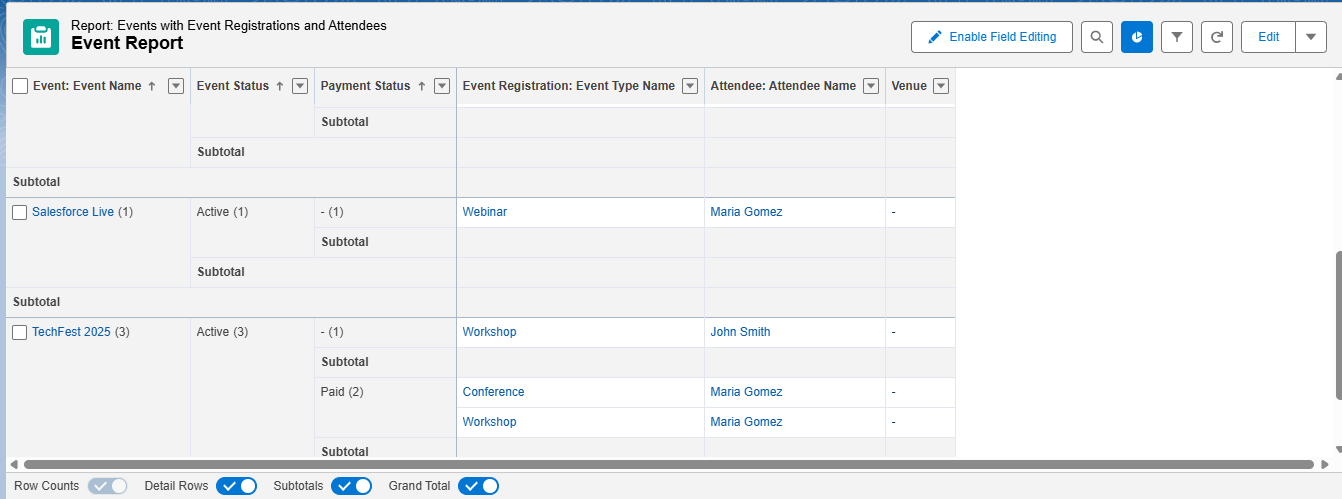
Provide actionable insights and maintain secure access by implementing robust reporting, dashboards, and security controls for the Event Management System.  
Focus on data visibility, metrics, user permissions, and audit trails.

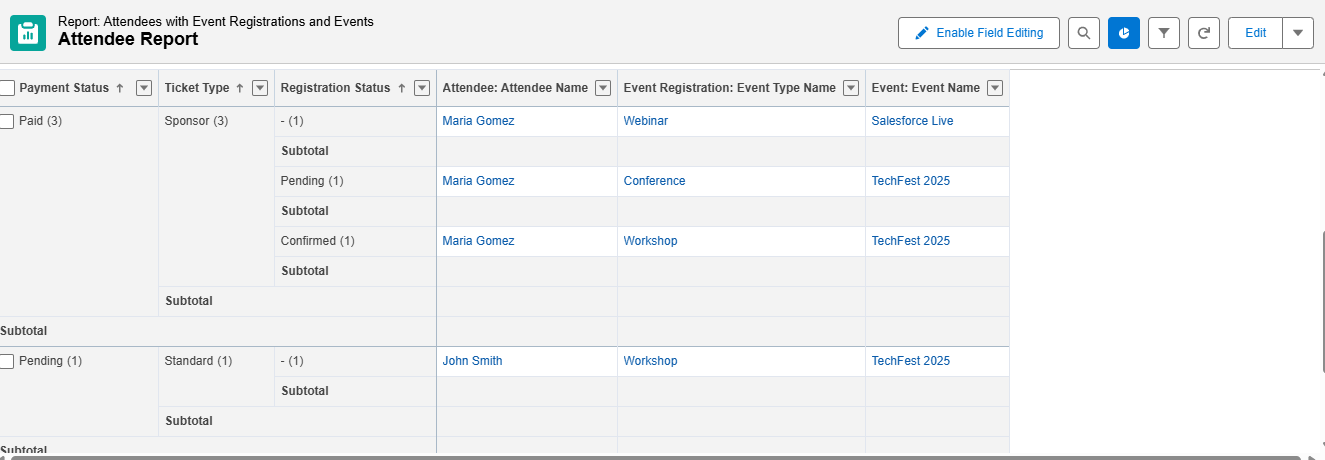
**1. Reports (Tabular)**

**Purpose:**  
Analyze and summarize event and attendee data to support decision-making.

**Report Types & Use Cases:**

* **Tabular Report:** List of upcoming events or attendee emails. Simple exportable data.



****

**Deliverables:**

* Predefined reports: Upcoming Events, Attendee Registration, Event Capacity Utilization.
* Shared report folders with access according to user roles.

**2. Report Types**

**Purpose:**  
Define the schema for custom reports with fields and relationships.

**Examples:**

* Custom Report Type: “Events with Attendees” (Event\_\_c → Attendee\_\_c)
* Standard Report Types: Accounts, Contacts (if applicable for venues or organizers)

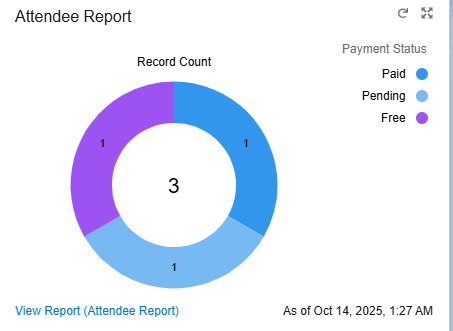
**Deliverables:**

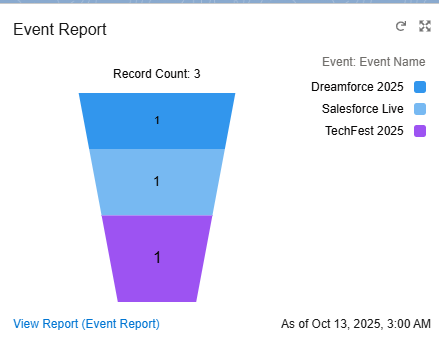
* Custom report types for Event Management objects.
* Documentation of field mappings and relationships.

**3. Dashboards**

**Purpose:**  
Provide visual summaries and KPIs for management and coordinators.

**Components:**

* Charts: Upcoming Events by Month, Attendee Registration Status.
* Gauges: Percentage of events fully booked.
* Tables: List of events with attendee counts.
* Dynamic filters: Allow selecting venue, organizer, or event type



**Deliverables:**

* Dashboard for Organizers: Event Summary, Registration Trends, Attendance Stats.
* Dashboard for Support/Management: Events needing approval, capacity alerts.

**4. Dynamic Dashboards**

**Purpose:**  
Allow users to view dashboards with data based on their access level (role hierarchy).

**Examples:**

* Organizer sees only their events.
* Event Manager sees all events across regions.

**Deliverables:**

* Dynamic dashboards configured for key roles.
* User testing for accurate data visibility.

**5. Sharing Settings**

**Purpose:**  
Control record visibility and access.

**Types:**

* **Organization-Wide Defaults (OWD):** Private, Public Read-Only, Public Read/Write.
* **Sharing Rules:** Grant access based on role, territory, or criteria.
* **Manual Sharing:** Ad-hoc record access for exceptions.

**Deliverables:**

* Documented sharing settings.
* Role hierarchy diagram.
* Active sharing rules.

**6. Field Level Security (FLS)**

**Purpose:**  
Control visibility/editability of sensitive fields.

**Examples:**

* Hide financial fields or attendee emails from standard users.
* Ensure only organizers and admins can edit event capacity.

**Deliverables:**

* Field-level security matrix.
* Verified access for each profile.

**7. Session Settings**

**Purpose:**  
Secure login sessions and enforce policies.

**Key Settings:**

* Session timeout: 30–60 minutes.
* Lock sessions to IP ranges (optional).
* Session security policies: Disable caching on public computers.

**Deliverables:**

* Configured session settings.
* Documentation of policies for compliance.

**8. Login IP Ranges**

**Purpose:**  
Restrict login access to trusted IP addresses for added security.

**Implementation:**

* Set trusted IP ranges for Salesforce org.
* Enforce IP ranges at profile level if needed.
* Monitor for login errors or exceptions.

**Deliverables:**

* IP range configurations per profile.
* Access review logs.

**9. Audit Trail**

**Purpose:**  
Track administrative and configuration changes for accountability and compliance.

**Use Cases:**

* Who changed sharing rules, reports, dashboards, or object metadata.
* Monitor login attempts and profile updates.
* Track changes to event data critical for compliance.

**Deliverables:**

* Setup audit trail reports.
* Periodic log downloads.
* Documentation of critical configuration changes.