**Phase 9 — Reporting, Dashboards & Security Review**

**1. Reports**

Salesforce provides different report formats to analyze data:

• Tabular Reports – Simple list of records. Example: All Leads created this month.

• Summary Reports – Grouped records with subtotals. Example: Leads grouped by Source or Counselor.

• Matrix Reports – Grouped by rows and columns. Example: Leads by Source vs. Owner.

• Joined Reports – Combine multiple report types into one view. Example: Leads and Enrollments for conversion tracking.

**2. Report Types**

• Standard Report Types – Provided by Salesforce (e.g., Leads, Accounts, Opportunities).

• Custom Report Types – Created for specific needs (e.g., Leads with Enrollments).

A screenshot of a computer

AI-generated content may be incorrect.

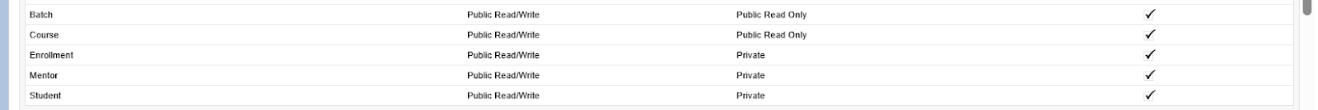
A graph showing a line

AI-generated content may be incorrect.

**4. Security Review**

**a. Sharing Settings**

Setup → Sharing Settings → Organization-Wide Defaults (OWD). Example: Leads = Private, Contacts = Controlled by Parent. Sharing rules can be defined to give managers access to counselors’ leads.



**b. Field Level Security**

Controls visibility and editability of fields for profiles and permission sets. Example: On Course object, Fees\_\_c field visible only to Admin/Manager, hidden from Counselors.

**c. Session Settings & Login IP Ranges**

• Setup → Security → Session Settings: Control session timeout, enforce HTTPS.  
• Login IP Ranges: Restrict logins to specific IP ranges (e.g., office network).

**d. Audit Trail**

Setup → View Setup Audit Trail. Tracks last 20 changes in setup (e.g., field creation, validation rules). Useful for governance an

A computer screen shot of a blue circle

AI-generated content may be incorrect.

**✅   Outcome**

• Comprehensive reporting with tabular, summary, matrix, and joined reports.  
• Dashboards created with key performance charts.  
• Dynamic dashboards provide role-based visibility.  
• Security implemented via OWD, FLS, IP restrictions, and audit trail.  
• CRM is analytics-ready and secure for client use.

**5. Sharing Settings**

Control who can view or edit records. Options include:

* **Private** – Records visible only to owners.
* **Public Read/Write** – Open visibility and edit rights.
* **Role Hierarchies** – Access cascades upward to managers/admins.

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

Restricts visibility or editability of sensitive fields (e.g., student phone numbers may be visible only to admins, not tutors).

**7. Session Settings**

Define login session timeouts, security levels, and multi-factor authentication policies to strengthen system security.

**8. Login IP Ranges**

Restrict logins to trusted networks (e.g., only within office IP ranges), minimizing unauthorized access risks.

**9. Audit Trail**

Tracks configuration changes (who changed what and when). Useful for compliance and troubleshooting.