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

1. **Reports (Tabular, Summary, Matrix, Joined)**

**Salesforce provides 4 main report formats:**

* **Tabular Reports** → Simple list of records (like an Excel sheet). Best for tasks like mailing lists.
* **Summary Reports** → Grouped by rows with subtotals (e.g., sales by region).
* **Matrix Reports** → Grouped by rows and columns; best for comparing data in two dimensions (e.g., sales by product vs. region).
* **Joined Reports** → Combine multiple report blocks with different objects into a single view. Useful for comparing related datasets.

1. **Report Types**

**Report Types** define the set of objects and fields available for reporting.

* **Standard Report Types** → Auto-created by Salesforce for common relationships (e.g., Accounts with Contacts).
* **Custom Report Types** → Created by admins for specific reporting needs, including custom objects and complex relationships.

1. **Dashboards**

**Dashboards** are visual representations of report data. They consist of components like charts, tables, gauges, or metrics. Dashboards give management quick insights into KPIs (e.g., total revenue, bookings, or charging station usage).

1. **Dynamic Dashboards**

**Dynamic Dashboards** allow users to see data based on their own security settings rather than the dashboard creator’s. For example, a Sales Manager sees only their team’s data, while an Operator sees only their assigned stations. This avoids creating multiple dashboards for different roles.

1. **Sharing Settings**

**Sharing Settings** define the default access (Organization-Wide Defaults) and record-level visibility. Admins can configure sharing rules for roles, groups, or territories. Sharing ensures that sensitive data is accessible only to authorized users.

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

**Field-Level Security** controls access to individual fields on objects. Admins can make fields **read-only**, **hidden**, or **editable** based on profiles/permission sets. This prevents exposure of sensitive information like payment details or customer PII.

1. **Session Settings**

**Session Settings** define how long a user session remains active before auto-logout, multi-factor authentication requirements, and session timeout warnings. Proper settings enhance security while balancing usability.

1. **Login IP Ranges**

Admins can restrict logins to specific IP ranges to enhance security. For example, internal users may only log in from corporate office IP addresses. This prevents unauthorized access from unknown networks.

1. **Audit Trail**

The **Setup Audit Trail** tracks configuration changes in Salesforce. It logs who made changes, what was changed, and when. This helps in compliance, troubleshooting, and monitoring unauthorized modifications.