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

In this phase, **WhatNext Vision Motos** leverages Salesforce’s analytics and security features to provide **real-time insights** and maintain a **secure environment**. Reports and dashboards empower decision-makers with actionable intelligence, while robust security practices ensure **data protection and compliance** across the mobility ecosystem.

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

* **Tabular Reports**: Simple listings such as *Vehicle Service Requests by Date*.
* **Summary Reports**: Aggregated data like *Total Revenue by Vehicle Model*.
* **Matrix Reports**: Multi-dimensional analysis (e.g., *Subscription Revenue by Region vs. Vehicle Type*).
* **Joined Reports**: Combine data from multiple report types, e.g., *Customer Engagement + Service History*.

**Report Types**

* Standard and custom report types created for specific business scenarios.
* Example: *Vehicles with Active Subscriptions* or *Customers with Expired Warranties*.

**Dashboards**

* Visual representation of KPIs for different departments.
* Example: A *Service Dashboard* showing open cases, turnaround time, and satisfaction scores.

**Dynamic Dashboards**

* Role-based dashboards showing personalized data.
* Example: Executives see **company-wide performance**, while sales reps see **their own pipeline and targets**.

**Sharing Settings**

* Organization-Wide Defaults (OWD), Role Hierarchies, and Sharing Rules ensure proper data access.
* Example: Service engineers see only their assigned cases, while managers see team-wide cases.

**Field Level Security (FLS)**

* Restricts sensitive fields like *Customer Payment Info* or *Vehicle IoT Data*.
* Ensures compliance with privacy and data protection standards.

**Session Settings**

* Configuring session timeouts, login hours, and re-authentication for enhanced protection.
* Example: Auto-logout after 15 minutes of inactivity for service kiosks.

**Login IP Ranges**

* Restrict access to Salesforce only from trusted networks.
* Example: Employees can log in from corporate VPN or office network, blocking unknown IPs.

**Audit Trail**

* Tracks configuration changes made by admins.
* Example: Logs when new sharing rules or profile updates are applied, ensuring accountability.