## **🧠 Workshop Assignment: Architecting an AI-Driven Support System with Agentforce**

Designing and Governing an Enterprise AI Support System — Lessons from Agentforce at Salesforce

### **🎯 Assignment Objective**

This assignment helps Enterprise Architects understand how to architect, govern, and scale AI-powered support systems using a case study of Agentforce. The goal is to explore data-driven automation, AI architecture layers, real-time orchestration, and trust mechanisms.

### **📋 Instructions**

1. **Case Review:** Read the Agentforce case study provided.
2. **Analysis Task 1:** Identify and document the key architecture components used to deliver Agentforce capabilities.
3. **Analysis Task 2:** Describe the enterprise architecture layers involved in integrating Agentforce with Data Cloud and Service Cloud.
4. **Design Task:** Propose a reference architecture for replicating a similar Agentforce solution for another company’s help center.
5. **Governance Task:** Define the governance and performance monitoring framework for such an AI system, addressing ethical, security, and operational aspects.

### **✅ Solution**

### **🧱 Task 1: Agentforce – Key Architecture Components**

| **Component** | **Description** |
| --- | --- |
| **Agentforce** | AI-powered agent layer handling 24/7 customer inquiries in natural language |
| **Data Cloud** | Unified customer data layer (structured + unstructured) for contextual AI |
| **Service Cloud** | CRM integration for ticketing, escalation, and case history context |
| **RAG (Retrieval-Augmented Generation)** | Powers precise, context-aware responses using real-time knowledge injection |
| **Natural Language Interface** | Supports free-form human questions without keyword matching |
| **Low-Code Builder** | Enables fast AI use case rollout, guardrail setup, and testing |

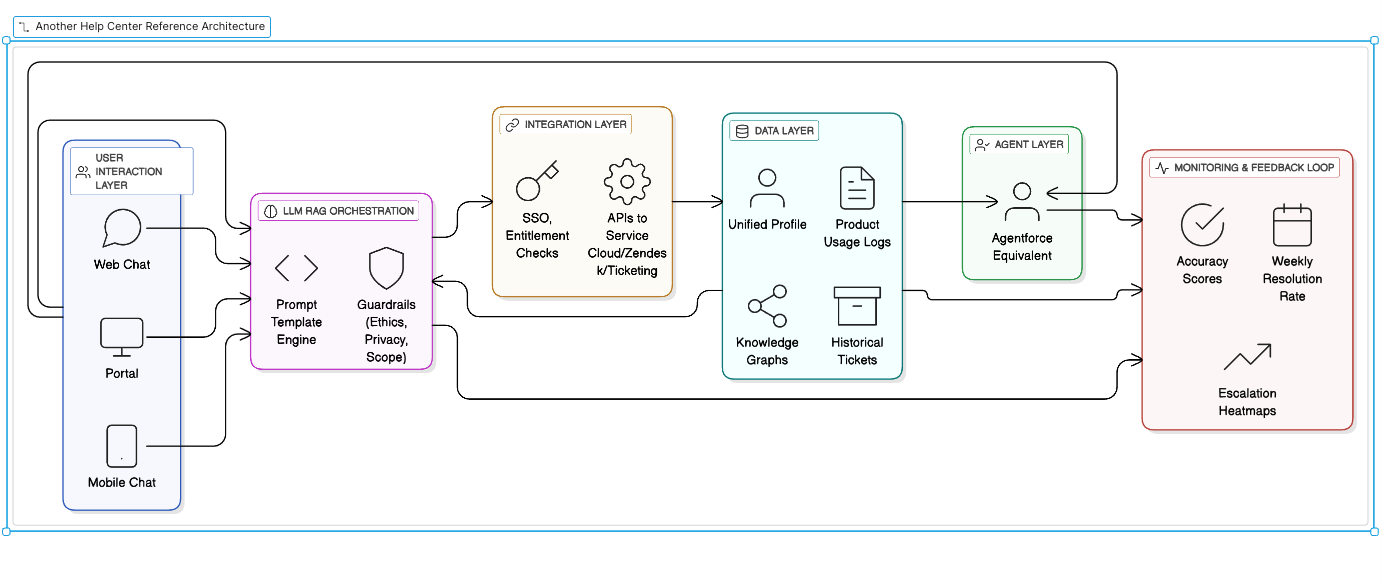
### **🧱 Task 2: Enterprise Architecture Layers Involved**

| **EA Layer** | **Role in Agentforce** |
| --- | --- |
| **Business Architecture** | Improves customer experience, reduces support costs, increases loyalty |
| **Application Architecture** | Integrates Agentforce with CRM, support tools, and chat interfaces |
| **Data Architecture** | Connects to Data Cloud (ID graphs, usage logs, knowledge base, etc.) |
| **Technology Architecture** | Hosts GenAI models, RAG pipelines, real-time APIs, low-code platform |
| **Security & Governance** | Implements TRiSM (Trust, Risk, Security Management) to monitor and control AI behavior |

### **📐 Task 3: Reference Architecture for Another Help Center**

**Architecture Diagram (summary description)**

1. **User Interaction Layer**
   * Web Chat / Mobile Chat / Portal
2. **Agent Layer (Agentforce Equivalent)**
   * LLM + RAG Orchestration
   * Prompt Template Engine
   * Guardrails (Ethics, Privacy, Scope Control)
3. **Integration Layer**
   * APIs to Service Cloud / Zendesk / Ticketing systems
   * SSO, Entitlement checks
4. **Data Layer (Data Cloud Equivalent)**
   * Unified Profile
   * Product Usage Logs
   * Knowledge Graphs
   * Historical Tickets
5. **Monitoring & Feedback Loop**
   * Accuracy Scores
   * Weekly Resolution Rate
   * Escalation Heatmaps



### **🛡️ Task 4: Governance and AI Trust Framework (TRiSM)**

| **Dimension** | **Governance Strategy** |
| --- | --- |
| **AI Ethics** | Human-in-the-loop escalation for complex/ambiguous cases |
| **Risk Control** | Red-flag topics auto-escalated; privacy masking of sensitive customer data |
| **Security** | Role-based access to customer context; compliance logging with GDPR/HIPAA controls |
| **Performance** | Weekly dashboards tracking % resolved, time to resolution, escalation rate |
| **Adaptability** | Continuous training on new documentation and updated product info |

### **📊 Key Metrics to Track (from Agentforce Benchmark)**

* ✅ **80%** of inquiries resolved without human agents
* ⚙️ **2x** the performance of previous bots
* 🔄 500,000+ conversations in first few weeks
* ⏱ **Seconds** to respond vs. **days** with traditional workflows

### **🧩 Bonus Prompt for EA Reflection**

"If you had to deploy Agentforce in your enterprise in 90 days, what foundational capabilities would you need to prioritize in data, access, and orchestration?"