cloudgaia | salesforce PARTNER

compliance agent | by cloudgaia

Post install setup & User guide

Table of content

1. Introduction 3
2. User Personas 3
3. Pre requisite & System requirements 3
4. Permissions & Access 4
    4.1 Assign Permission Sets 4
    4.2 Einstein AI Permissions 4
5. Features Activation (Einstein AI) 5
    5.1. Step 1: Turn on Einstein Generative AI 5
    5.2. Step 2: Activate the Compliance Agent Prompt Template 6
6. Security Note: Built in Data Protection 6
7. Post installation checklist 7
    7. 1. Configure 'Setting' Custom Metadata 7
    7. 2. Configure 'Context' Custom Metadata 9
    7.3. Define Target Fields for analysis 10
    7.4. Assign the 'Compliance Agent' Tab 11
    7.5. Add the LWC to Lightning Pages 12
8. Step by step user guide 13

1. Introduction

Welcome to Compliance Agent

Compliance Agent addresses a silent but costly operational risk that many organizations face every day: the disconnect between signed legal documents and the actual data living inside Salesforce. We consistently see teams wasting valuable time reading a contract on one screen while manually checking fields on another just to ensure everything aligns. This application changes that entirely by automatically reading the document clauses and comparing them directly against your live CRM records. What truly sets this solution apart is how it transforms compliance from a reactive chore into a proactive safeguard. By instantly catching mismatches in payment terms, service level agreements, and expiration dates, you prevent minor data entry errors from turning into significant financial or legal liabilities. It guarantees that your billing and daily operations strictly honor your legal commitments. Ultimately, implementing this tool gives your users their time back, allowing them to step away from tedious paperwork audits and focus on the strategic work that actually drives your business forward. This guide provides everything you need to configure the application and start seeing this value immediately.

2. User Personas

To ensure a secure and efficient workflow, the Compliance Agent is designed around two primary user profiles, each with distinct responsibilities:

System Administrator (Manager): The technical or compliance lead responsible for installing the application, configuring the AI mapping rules (Custom Metadata), and maintaining global oversight of all compliance audits.

End User: The everyday business operator, such as an Account Executive or Contract Manager, who interacts with the application to analyze PDF contracts and review the AI generated discrepancies directly within their standard Salesforce workflow.

3. Pre requisite & System requirements

Before you install and configure Compliance Agent, make sure your Salesforce org meets these minimum requirements:

- **Salesforce Edition**: You must be on Enterprise, Performance, or Unlimited Edition. (The app relies on advanced metadata and AI features that are not fully supported in Professional Edition).
- **Einstein Generative AI:** Your org must have Einstein Generative AI enabled. This means you need access to Prompt Builder, which is typically included in the Einstein 1 editions (Sales, Service, or Platform) or available via an Einstein add on license.
- **Lightning Experience:** The Compliance Agent component is built exclusively for Lightning record pages and cannot be used in Salesforce Classic.

4. Permissions & Access

4.1 Assign Permission Sets

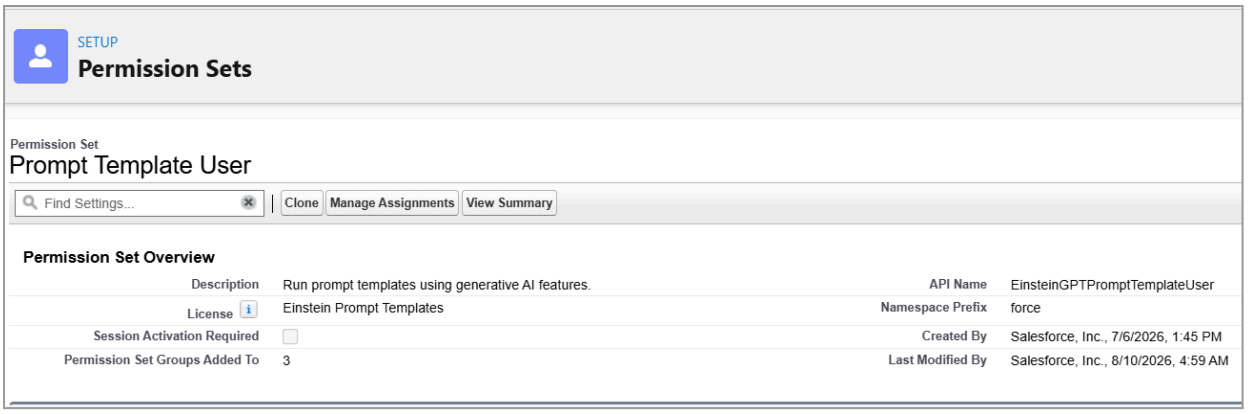
Compliance Agent leverages standard Salesforce security. To grant access, simply assign one of the following two role-based Permission Sets depending on the user's objective:

- **Compliance Agent User:** Assign this to your standard business users who need to use the tool in their daily workflow. It provides the exact baseline permissions required to execute a contract analysis and view the generated *Compliance Review* results.
- **Compliance Agent Manager:** Assign this to System Administrators or Compliance Team Leads. It provides elevated privileges to configure the application's AI mapping rules (Custom Metadata) and grants full global visibility to oversee and audit all *Compliance Review* records across the organization.

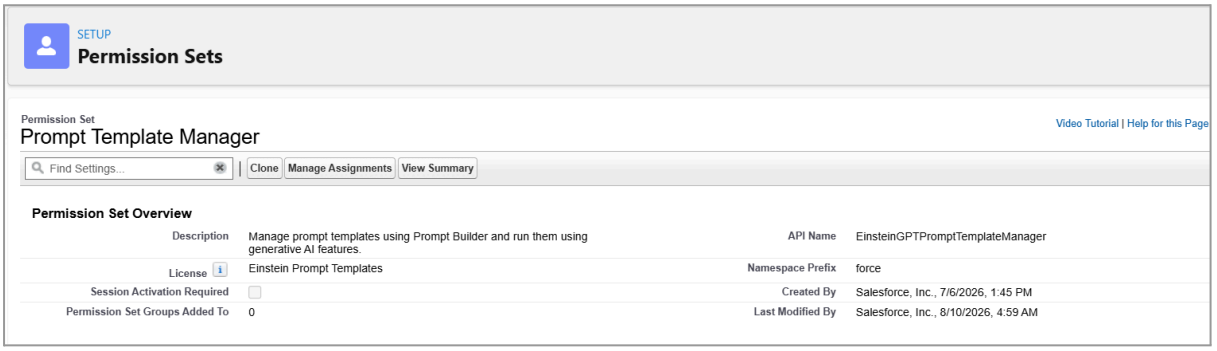
4.2 Einstein AI Permissions

Because **Compliance Agent** uses standard Salesforce AI capabilities, your users must have permission to execute prompts. Make sure they are assigned the standard **Prompt Template User** (for end user) and **Prompt Template Manager** (for Admin).

End User



Administrators/Managers



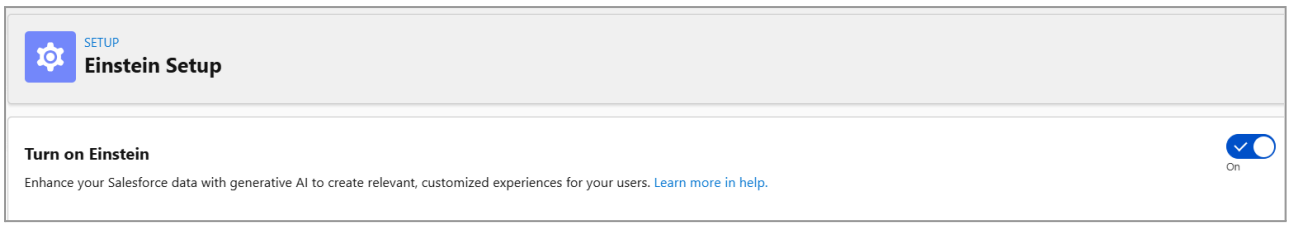
5. Features Activation (Einstein AI)

Before **Compliance Agent** can start reading and analyzing contracts, you need to "wake up" the AI in your Salesforce org. Since the app relies entirely on Salesforce's native AI engine, here is the step by step to get Einstein up and running.

5.1. Step 1: Turn on Einstein Generative AI

First, we need to make sure Salesforce is allowed to generate AI responses in your environment.

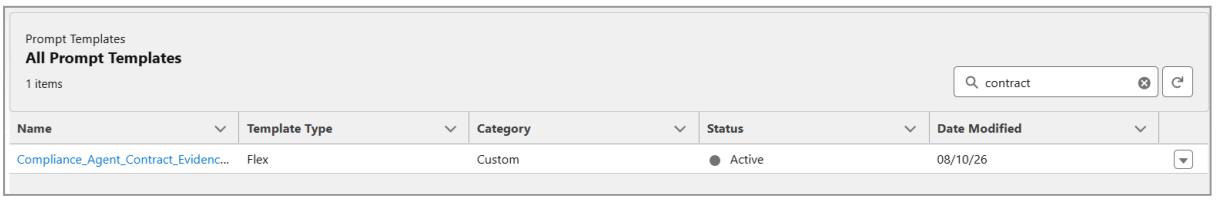
1. Go to **Setup** (the gear icon).
2. In the Quick Find box, type **Einstein Setup.**
3. Toggle the switch to **Turn on Einstein**. *(If it's already on, you can skip this step!)*



5.2. Step 2: Activate the Compliance Agent Prompt Template

The app comes with a pre packaged Prompt Template (this is the secret sauce that tells the AI exactly how to cross reference the PDFs with your Salesforce fields). It usually installs in an "Inactive" state, so you need to flip the switch.

1. In **Setup**, go back to **Prompt Builder.**
2. Find the template named **Compliance_Agent_Contract_Evidence_Analysis** in the list and click on it.
3. In the top right corner, click **Activate**.





6. Security Note: Built in Data Protection

By enabling Einstein Generative AI, your Salesforce org is automatically protected by the **Einstein Trust Layer**. You do not need to perform any additional setup to secure your data. This native security shield operates in the background to ensure:

- **Zero Data Retention:** Your contract data and Salesforce records are never stored by external LLM providers.
- **No Model Training:** Your private information is never used to train outside artificial intelligence models.
- **Data Masking:** Sensitive information is protected before leaving your Salesforce environment.

7. Post installation checklist

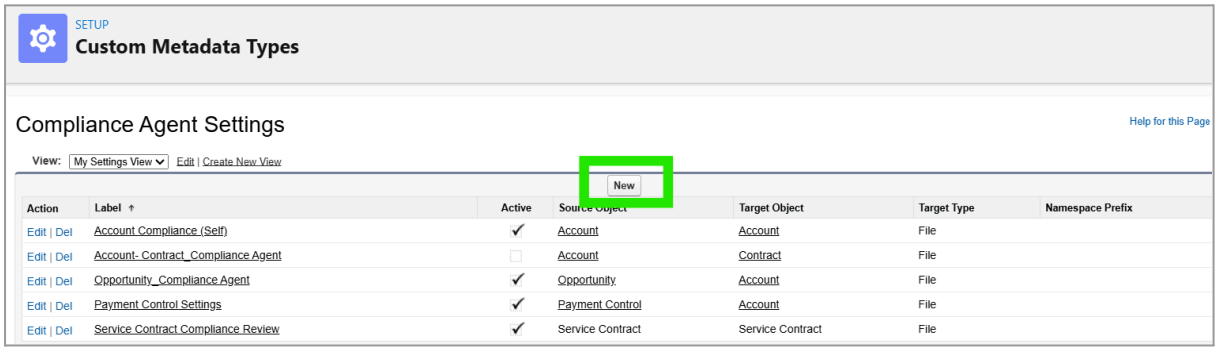
Once the package is installed and the permissions are assigned, you need to tell Compliance Agent exactly how to behave in your unique Salesforce environment. Follow these 5 steps to activate the agent:



7. 1. Configure 'Setting' Custom Metadata

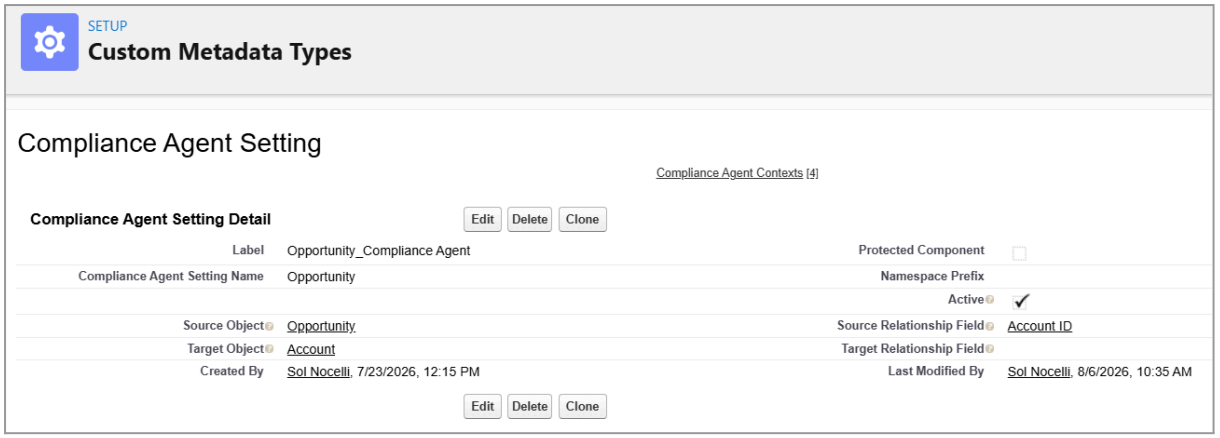
This is the foundational configuration where you define the global rules for the application.

What to do:
Navigate to **Setup** > **Custom Metadata Types** and find the Setting metadata type for Compliance Agent **(Compliance_Agent_Setting__mdt)**. Click **Manage Compliance Agent Settings** and then **New** to create your default configuration.



Why it matters:

This configuration establishes the starting point and endpoint of your validation process. You must set this up to tell the system exactly where the component is located (the **Source**) and define where it should look to find the master data (the **Target**) for its analysis.



Compliance Agent Setting: Fields Definitions

Label: The readable name of this configuration record. It is a best practice to name it clearly (e.g., [Source Object]_Compliance Agent) so you can easily identify it in a list view.

Compliance Agent Setting Name: The unique API name for this metadata record. This is generated automatically based on the Label and is used by the system's backend code to query this specific setting.

Source Object: Defines the starting point of the validation. This must be the API Name of the object where the Lightning Web Component (LWC) is physically placed (e.g., Opportunity).

Target Object: Defines the endpoint of the validation. This is the object where the master data resides and where the system should look for the contract document and related records data in Salesforce (e.g., Account).

Active: A checkbox that determines if this configuration is currently running. If unchecked, the Compliance Agent component will not execute on the defined Source Object, allowing you to temporarily disable the feature without deleting the configuration.

Source Relationship Field: The API name of the lookup or master detail field on the *Source Object* that connects it to the *Target Object*. For example, if the LWC is on the Opportunity and needs to read the Account, this field must contain AccountId.

Target Relationship Field: This is used for more complex data models where you need to specify a reverse lookup or a specific relationship path on the target side. If the *Source Relationship Field* already establishes a direct link, this can be left blank.

Protected Component & Namespace Prefix: Standard Salesforce packaging fields. *Protected Component* hides the record from managed package subscribers (leave

unchecked for End User orgs), and *Namespace Prefix* is populated automatically if the app is distributed via a managed package.

7. 2. Configure 'Context' Custom Metadata

This Custom Metadata Type defines the related objects and specific fields the Compliance Agent needs to query to build the context for the AI analysis.

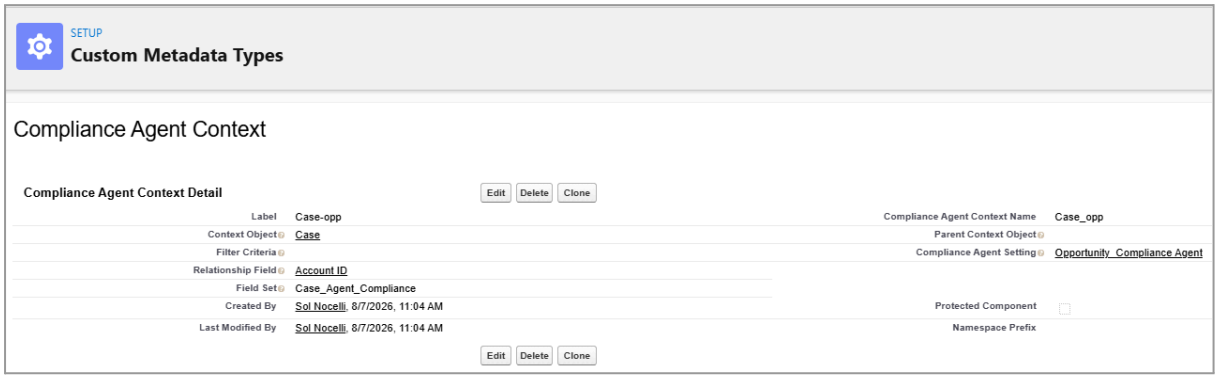
What to do:

In **Setup** > **Custom Metadata Types**, find the **Compliance Agent *Context*** metadata type and click **Manage Compliance Agent Records**.

Create a new record for each Salesforce object where you want to use the agent.

Why it matters:

Properly configuring the **Compliance Agent Context** via Custom Metadata Types is the most critical step in your setup process. This configuration acts as the intelligent bridge between your structured Salesforce CRM data and the unstructured text within your PDF contracts.



Compliance Agent Context: Field Definitions

Label: The user friendly name for recognize the setting

Compliance Agent Context Name: The user friendly name and the unique API name for this metadata record. It is recommended to use a naming convention that clearly identifies the relationship being mapped (e.g., Case_opp to denote Cases related to the main Opportunity).

Context Object: The exact Name of the Salesforce Object that contains the data to be analyzed (e.g., Case, Account, Custom_Object__c). The Apex controller will query this object to gather context.

Filter Criteria: Optional. A SOQL compliant filter condition used to restrict which records are retrieved from the Context Object. For example, to only analyze closed cases, you could input Status = 'Closed'. Leave blank to retrieve all related records.

Relationship Field: The API Name of the lookup or master detail field on the *Context Object* that connects it to the primary object where the Lightning Web Component is running (or to the Parent Context Object). For example, if querying Cases related to an Account, this would be AccountId.

Field Set: The exact API Name of the standard or custom Field Set created on the *Context Object*. The Compliance Agent relies on this *Field Set* to know exactly which specific fields (and their values) must be extracted, formatted into JSON, and sent to the LLM for the compliance review.

Parent Context Object: Used for supporting hierarchical data retrieval. If the data model requires traversing multiple levels of relationships, this field holds the Name of the parent object in that hierarchy. Leave blank if the Context Object is directly related to the main record.

Compliance Agent Setting: A relationship field that links this context record back to the primary/master "Compliance Agent Setting" record. This defines which overarching configuration this specific object context belongs to.

Protected Component: A standard Salesforce configuration flag. When checked, this prevents the metadata record from being modified in subscriber orgs (typically managed by the ISV during package creation).

7.3. Define Target Fields for analysis

The AI needs to know exactly which data points in Salesforce it should compare against the PDF contract.

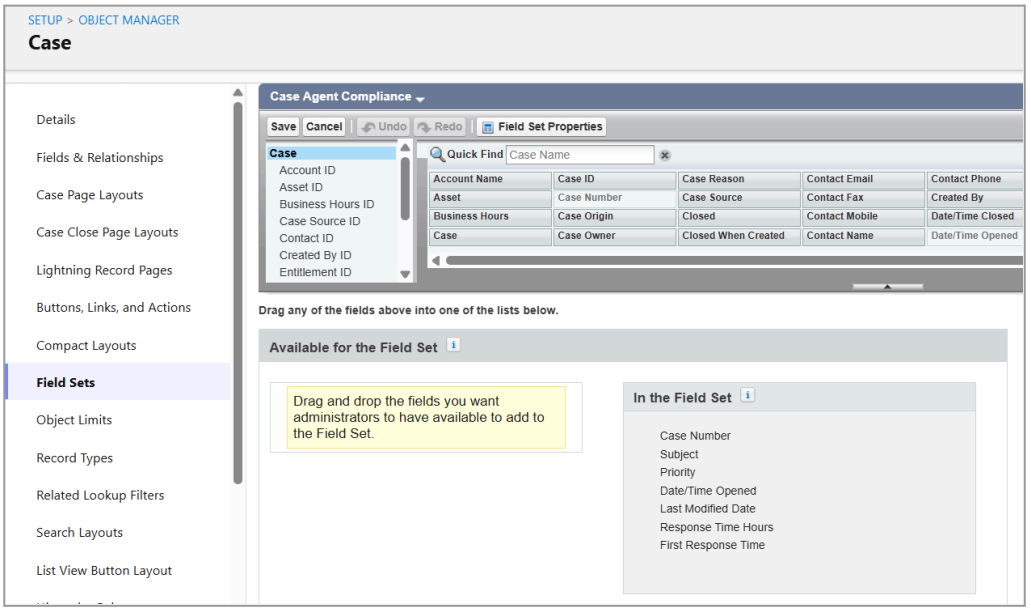
What to do:

Go to the Object Manager for your chosen context object (e.g., Case). Create or locate the specific Field Set designated for Compliance Agent, and drag and drop the relevant fields into it.

Why it matters:

Think of the Field Set as the specific checklist you are giving to the AI. The AI will only cross reference the data points you explicitly include in this set. For example, if you need the AI to verify SLAs, those exact fields (e.g., First_Response_Time__c and Response_Time_Hours__c) must be added to the Field Set.

The golden rule: If a field is not included in the Field Set, the AI is completely blind to it and will ignore it during the analysis.



7.4. Assign the 'Compliance Agent' Tab

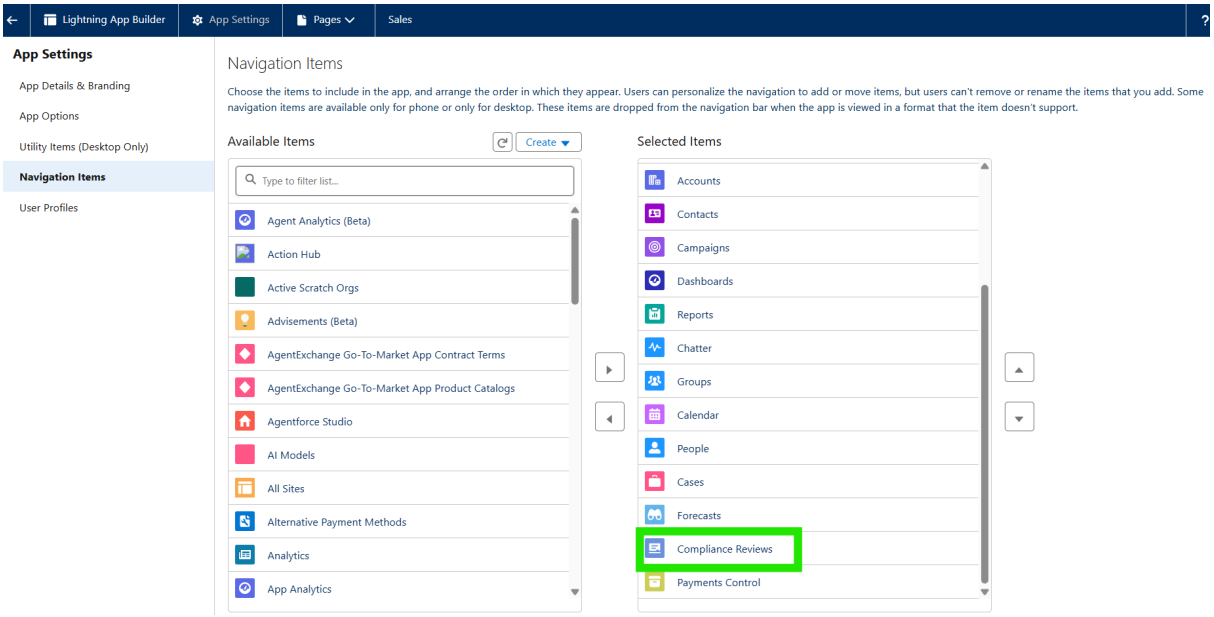
Every time the agent analyzes a contract, it saves the findings as a unique record so you have a complete audit history. You need to make this repository visible to your users.

What to do:

Go to **Setup** > **App Manager**. Edit the **Lightning Apps** your team uses (like the standard *Sales* app) and add the **Compliance Review** tab to the **Navigation Items**.

Why it matters:

This allows managers and compliance officers to view a centralized list of all historical discrepancies found across all analysis.



7.5. Add the LWC to Lightning Pages

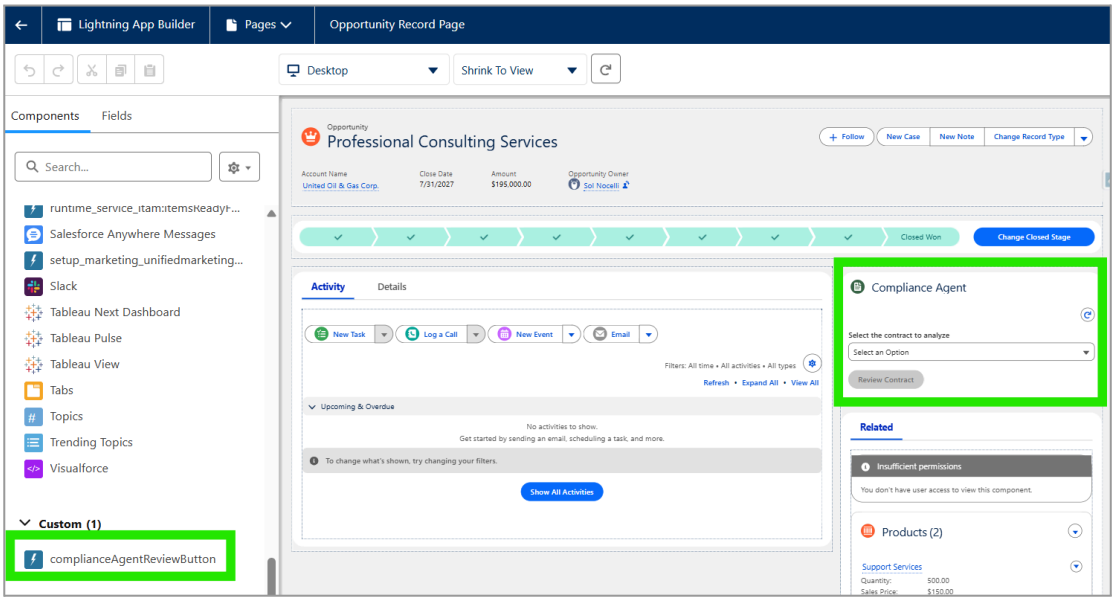
The final step is to put the tool exactly where your users do their work.

What to do:

Open a record page where you want the agent to live (for example, an Opportunity record). Click the **gear icon** and select **Edit Page** to open the Lightning App Builder.

Action: Drag the custom Compliance Agent Lightning Web Component (LWC): *'ComplianceAgentReviewButton'* from the left sidebar and drop it onto your page layout. Click **Save** and **Activate**.

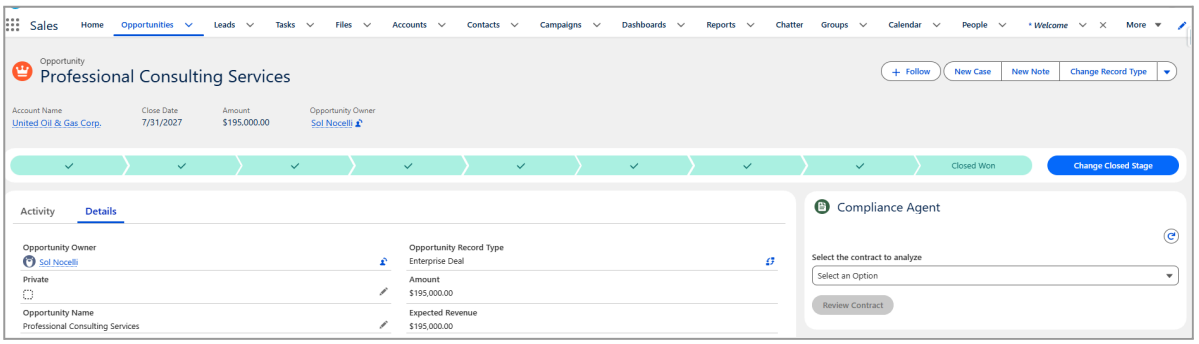
Finally, the users are now ready to start analyzing contracts.



8. Step by step user guide

Using the Compliance Agent is designed to be a seamless and intuitive experience directly within your standard workflow. Follow these simple steps to perform a contract review:

1. **Navigate to the Record:** Go to the specific Salesforce record (such as an Account, Opportunity, Case or any custom object) where the contract analysis needs to take place, and locate the **Compliance Agent** component on the page.



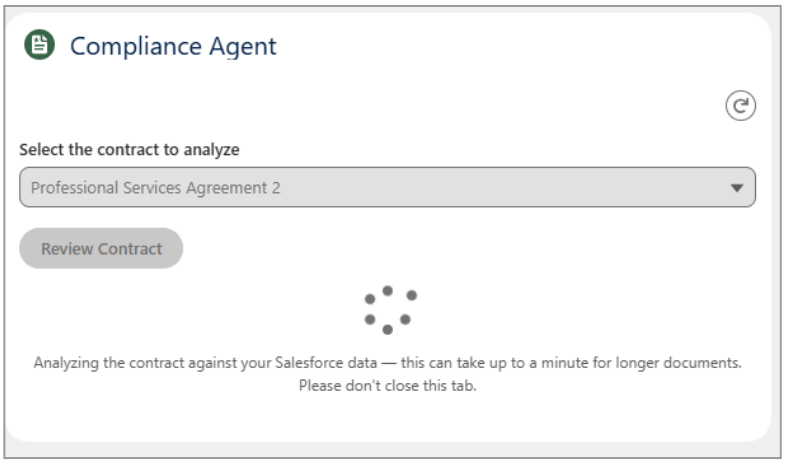
2. **Select the Document:** Inside the component, click the picklist (dropdown menu) and select the attached PDF contract or file you wish to analyze.



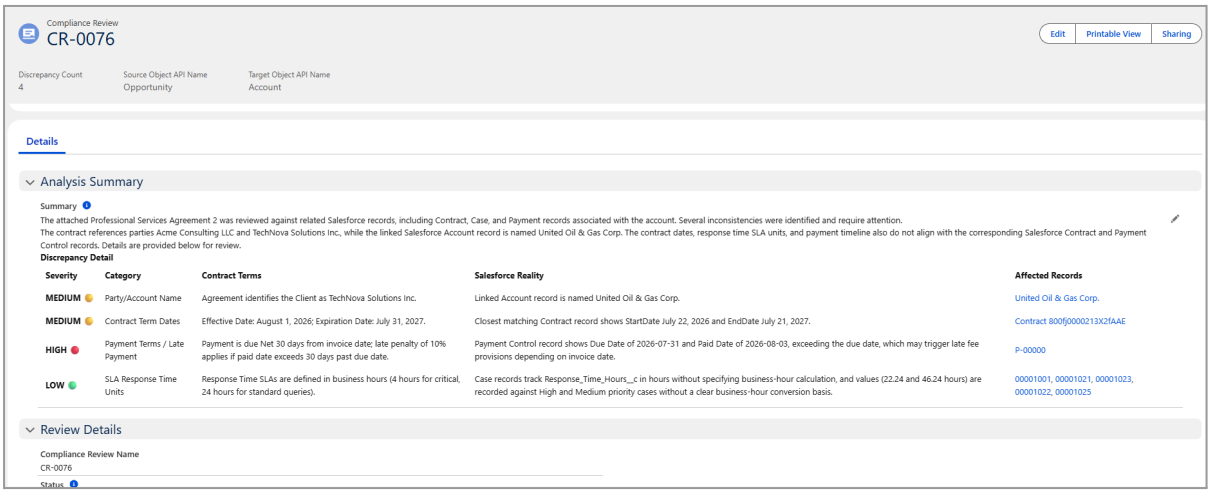
3. **Initiate the Analysis:** Click the **"Contract Review"** button to start the AI evaluation.

4. **Allow for Processing:** A loading spinner will appear on your screen. This indicates that the application is actively working in the background, cross referencing the

clauses in your selected document against the live data fields currently residing in your Salesforce CRM.



5. **Review the Results:** Once the analysis is complete, the application will automatically redirect you to a newly created **Compliance Review** record. This screen will display the full results of the audit, clearly highlighting any discrepancies found between the external document and your system data.

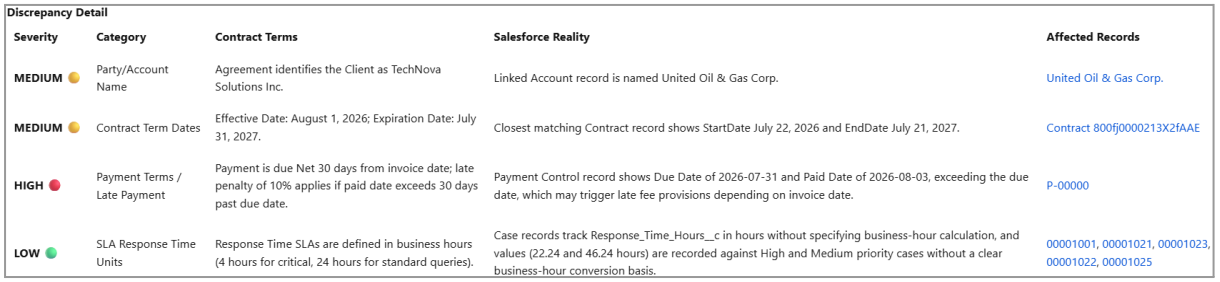


This page is designed to give you both a high level overview and actionable, granular data.

Analysis Summary:

At the top of the page, you will find a brief narrative paragraph. This serves as an executive summary, explaining which records were checked and summarizing the overarching inconsistencies (e.g., mismatched account names or SLA discrepancies) in plain language.

Discrepancy Detail Table:



Discrepancy Detail

Severity	Category	Contract Terms	Salesforce Reality	Affected Records
MEDIUM	Party/Account Name	Agreement identifies the Client as TechNova Solutions Inc.	Linked Account record is named United Oil & Gas Corp.	United Oil & Gas Corp.
MEDIUM	Contract Term Dates	Effective Date: August 1, 2026; Expiration Date: July 31, 2027.	Closest matching Contract record shows StartDate July 22, 2026 and EndDate July 21, 2027.	Contract 800fj0000213X2fAAE
HIGH	Payment Terms / Late Payment	Payment is due Net 30 days from invoice date; late penalty of 10% applies if paid date exceeds 30 days past due date.	Payment Control record shows Due Date of 2026-07-31 and Paid Date of 2026-08-03, exceeding the due date, which may trigger late fee provisions depending on invoice date.	P-00000
LOW	SLA Response Time Units	Response Time SLAs are defined in business hours (4 hours for critical, 24 hours for standard queries).	Case records track Response_Time_Hours__c in hours without specifying business-hour calculation, and values (22.24 and 46.24 hours) are recorded against High and Medium priority cases without a clear business-hour conversion basis.	00001001, 00001021, 00001023, 00001022, 00001025

Below the summary, a detailed table breaks down every specific issue the AI detected. Pay close attention to these columns:

- **Severity:** Color coded indicators (High, Medium, Low) help you immediately prioritize which discrepancies pose the greatest business or compliance risk.
- **Category:** Identifies the specific business area of the mismatch (e.g., Payment Terms, Contract Dates, or Account Name).
- **Contract Terms vs. Salesforce Reality:** This side by side comparison shows exactly what is written in the uploaded PDF document versus what data currently exists in your live Salesforce system.
- **Affected Records:** Provides direct, clickable links to the specific Salesforce records containing the mismatched data, allowing you to navigate instantly to the source and correct it.