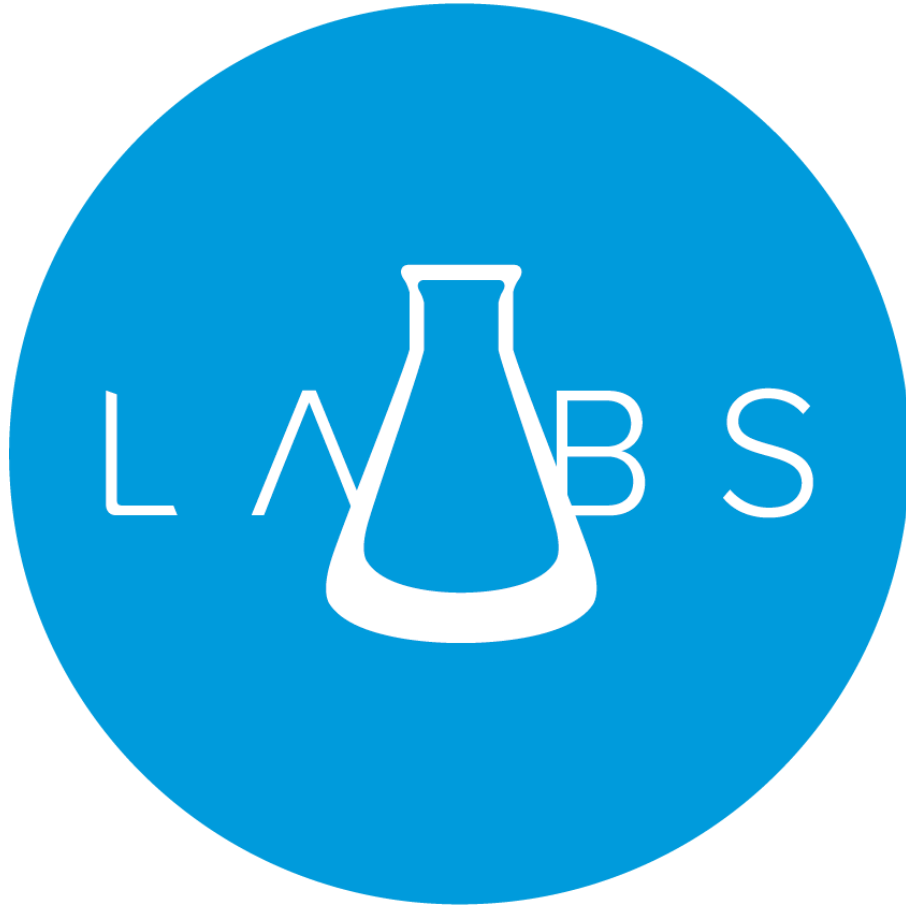


AI Governance App ver 0.3

ver 0.3

Set Up and User Guide



Create. Innovate. Educate.

Introduction

Welcome to the AI Governance and Management App, your comprehensive solution for overseeing AI initiatives within your organization. This app is designed to provide a robust framework for documenting, tracking, and managing various aspects of AI development and deployment. With a focus on transparency, compliance, and strategic alignment, this app offers a range of features to support your AI governance needs.

Key features include AI Use Case documentation, where you can capture detailed information about each AI initiative, including

an overview, objectives, expected outcomes, and regulatory evaluation considerations. This ensures a thorough understanding of the purpose and impact of each AI project.

The app also facilitates comprehensive data management by allowing you to document and classify data sources, including details on data impact levels, structured formats, and ownership. This supports proper data governance and compliance with regulatory standards.

AI Feature cataloging is another key component, enabling easy tracking and association of AI features with relevant use cases. This helps manage the capabilities and functionalities deployed across various projects.

Additionally, the app provides tools for model and endpoint tracking, where you can store information about AI models, including versions, training data, and risk assessments. It also manages AI endpoints by capturing details like URLs, request limits, and compliance standards.

Risk and stakeholder management features allow you to document potential risks associated with AI Use Cases and maintain a list of stakeholders, linking them to specific data sources and use cases. This ensures that all relevant parties are engaged and that risks are properly evaluated and mitigated.

The concept of Compliance Checklists have been introduced to provide a structured set of questions for each use case, which can then be assigned to individual stakeholders. This approach ensures that use cases are consistently evaluated against a predefined set of standard questions.

The AI Application Implementation feature enables you to manage the implementation of AI applications that incorporate multiple use cases, providing a unified view of the integration and deployment of AI technologies within specific applications.

Finally, the app supports feedback and test case management, allowing you to collect and manage feedback and test cases to support continuous improvement and validation of AI models and features.

This app serves as a centralized platform for all your AI governance needs, providing a clear and structured approach to managing AI projects. By consolidating information and streamlining processes, it enables effective oversight, compliance, and strategic decision-making in AI development and deployment.

* [Salesforce Labs provides free, open source solutions to the AppExchange.](#)

System requirements:

Available for use in Enterprise, Unlimited, Force.com, Developer, and Performance Editions of Salesforce.

The AI Governance App is a free solution designed to optimize the user experience with the following Salesforce Products, and thus requires

- Platform License

Installation Guide

*Some Labs developers include a step by step guide of installing your solution from AppExchange. While this is not required, it may be helpful for users who are new to AppExchange.

Login with your trailhead email and navigate to our listing on Appexchange <link>

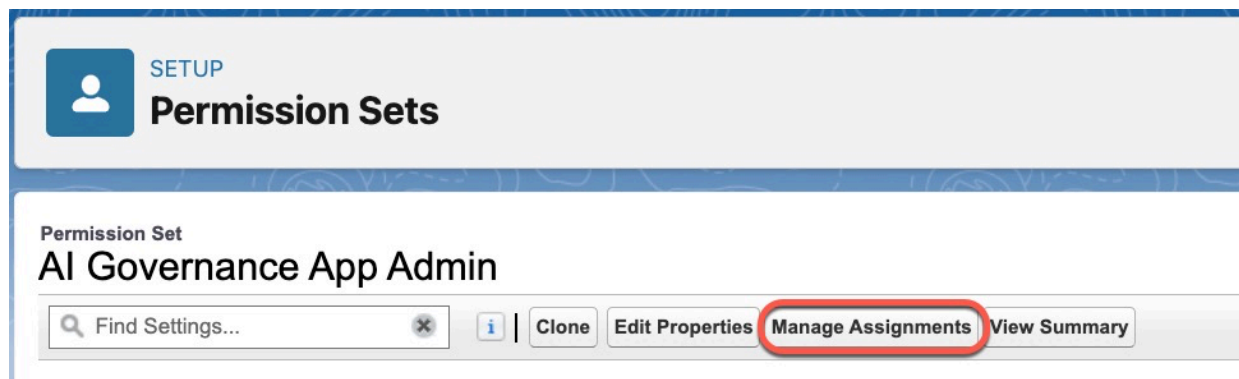
Select “Get it Now” from the listing and select the org you want to install it in from the drop down

1. Agree to the terms and conditions
2. **Select “Get it Now” from the listing and select the org you want to install it in from the drop down**
3. Agree to the terms and conditions
4. Once you have redirected to the Salesforce login page, input the credentials for the Salesforce org you wish to install the solution in
5. Select the profiles you wish to access the solutions (Admins Only, Everyone, or Specific Profile>)

Set Up Guide

ASSIGN PERMISSION SET

Once the package is installed, provide access to users via the **AI Governance App Admin** permission set.



AI GOVERNANCE APP

On the **Home** page for the **AI Governance App**, begin the configuration by populating the data for:

- AI Models
- AI Data Sources
- AI Endpoints
- AI Features
- AI Stakeholders
- AI Compliance Checklists

AI MODEL

Add the applicable AI Models for your organization. This designed to store and manage comprehensive information about AI models used within an organization. This object serves as a central repository for details about each AI model, including its identity, version history, training data specifics, and associated risk assessments.

A Risk Scorecard component has been incorporated, which evaluates the potential risks associated with each model. This scorecard is tailored to the organization's unique risk tolerance framework, providing a standardized method to assess and manage the risks inherent in deploying AI technologies. The risk scorecard facilitates informed decision-making by highlighting

areas of concern and enabling proactive risk mitigation strategies.

Q Search...

AI Governance

AI Models

OpenAI GPT-4 | AI ...

AI Model

OpenAI GPT-4

EditCloneDelete

RelatedDetails

Model Information

AI Model Name	Training Data As Of
OpenAI GPT-4	9/1/2021
Version	Status
gpt-4-0613	Evaluating for Use

Considerations

Suggested Use

GPT-4 outperforms both previous large language models and as of 2023, most state-of-the-art systems (which often have benchmark-specific training or hand-engineering). GPT-4 is optimized for chat but works well for traditional completions tasks using the Chat Completions API.

Ethical Considerations

Inaccurate outputs from GPT-4 could contribute to the spread of misinformation, perpetuating biased narratives and reinforcing harmful stereotypes. Addressing biases in training data becomes crucial to mitigate these potential downsides

Risk Scorecard

Data Privacy Risk

High

Model Bias Risk

Moderate

Regulatory Compliance Risk

Moderate

External Risk Scorecard URL

Provider Information

Provider

OpenAI

Provider Site

https://openai.com/

Additionally, you can create a workflow to route approvals for various models. When selecting a model for an AI Use Case, only those models with the status of 'Evaluating for Use' or 'Approved for Use' will be available for display.

AI DATA SOURCE

Serves as a comprehensive repository for information related to the data sources utilized in AI models and applications. This object captures key details about each data source, including its classification, data impact level, type, and origin. It specifies whether the data is structured or unstructured and provides the relevant object/table and field/column details for structured data.

AI Data Source

Customer Transaction Data

EditCloneDelete

Data Impact Level

Low

Classification

Restricted

RelatedDetails

▼ Data Source Information

Data Source Name	Customer Transaction Data	Classification	Restricted
Type	Structured	Data Impact Level	Low
Origin	Internal		

▼ Data Format Details

Structured Format	Database	Object/Table	Customer
		Field/Column	

▼ Data Source Owner

Data Owner

AI FEATURE

AI Features are designed to catalog and document individual features of AI systems. It serves as a comprehensive repository for AI features that can be associated with various AI Use Cases. This object enables organizations to track, manage, and analyze AI capabilities across different projects and applications.

AI Feature

Einstein Copilot

EditDelete

Description

Einstein Copilot handles questions posed by users in natural language and provides relevant answers drawn from secure, proprietary co...

AI Type

Generative

Owner

▼ Details

AI Feature Name	Einstein Copilot
AI Type	Generative
Description	Einstein Copilot handles questions posed by users in natural language and provides relevant answers drawn from secure, proprietary company data.
License Information	Enterprise, Performance, and Unlimited Editions with the Einstein for Sales, Einstein for Service, or Einstein Platform add-ons

Use Cases (0)

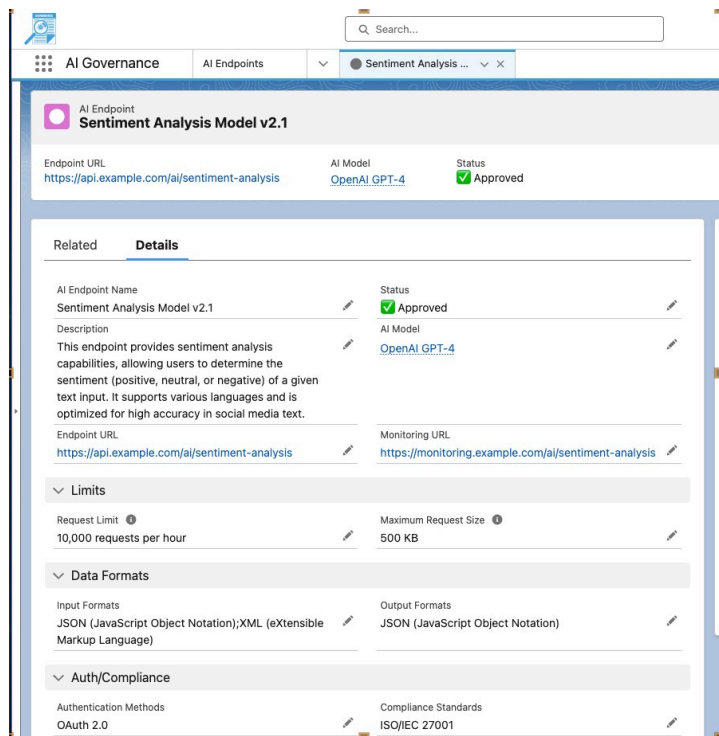
New

AI ENDPOINT

Designed to catalog and manage details about the endpoints through which AI models are accessed and utilized. This object provides a comprehensive overview of each AI endpoint, including its operational status, associated AI model, and technical specifications. It captures essential information such as the endpoint URL, monitoring URL, request limitations, and data format

requirements for both input and output. Additionally, the object includes details about the authentication standards and compliance requirements that must be met when interacting with the endpoint.

A vital resource for developers, system integrators, and compliance officers, ensuring that all necessary technical and regulatory aspects are documented and accessible. By maintaining a clear and detailed record of each AI endpoint, this object supports efficient integration, monitoring, and management of AI services within an organization's IT infrastructure.



AI STAKEHOLDER

Designed to manage and document the stakeholders involved in AI projects, specifically those related to data sources and use cases. This object captures their association with either a Salesforce contact (from the standard Contact object) or a Salesforce user. It serves as a centralized record of all individuals or entities that have a vested interest in the AI initiatives within the organization.


AI Stakeholder
Bryan Wise

Related
Details

Information

AI Stakeholder Name
Bryan Wise

Contact

User
 Bryan Wise

Owner
 Jen McClure

AI COMPLIANCE CHECKLIST

Compliance Checklists were designed to allow a grouping of questions to be associated to Individual AI Use Cases, these are stored in the AI Use Case Risk object..


AI Governance
Home
Recently Viewed | A...
UC-0000000 | AI U...
2024 Executive Ord...

2024 Executive ...
9-9999...

AI Compliance Checklist Question
Q-0000000

Question
Was the AI system involved in this use case developed (or is it to be developed) under contract(s) or in-house?

Active
☒

Details

Question
Was the AI system involved in this use case developed (or is it to be developed) under contract(s) or in-house?

Configuration

Response Type
Multiple Choice

Category

Active
☒

Default Decision Maker

AI Compliance Checklist Resp Choices (2)
2 items - Updated a few seconds ago

☐ Choice Label

Impact

Likelihood

1 ☐ In-house

2 ☐ Under Contracts

View All

Compliance Checklist Questions may have 2 types of responses:

- Text
- Multiple Choice

When defining a Multiple Choice Question, input the possible choices along with the optional **Impact** and **Likelihood** for each response. If these values are provided, they will automatically apply to the use case risk when a user selects that response. Additionally, you can specify a **Default Decision Maker** to be automatically associated with this question for the use case.


AI Compliance Checklist Question
Q-0000007

Question

What is the status from the CISO's office?

Active ☒

Details

Question

What is the status from the CISO's office?

Configuration

Response Type

Multiple Choice

Active ☒

Category

Default Decision Maker


AI Compliance Checklist Resp Choices (2)

⚙️

🔄

New

2 items • Updated a few seconds ago

	Choice Label	Impact	Likelihood	
1	☐ Approved	● Very Low Impact	■ Likely	▼
2	☐ Needs further evaluation	● High	■ Possible	▼

AI USE CASE

The setup is now complete, and you can begin documenting the **AI Use Cases**. This section provides a structured framework for capturing comprehensive information about each AI Use Case, including an overview, detailed description, objectives, expected outcomes, and regulatory evaluation considerations.

For each AI Use Case, you can link multiple related components, such as AI Features, Data Sources, AI Models, Endpoints, Risks, Stakeholders, Test cases, and Feedback. This comprehensive documentation helps in understanding the scope, impact, and compliance requirements of each use case.

By maintaining detailed records of all aspects of an AI Use Case, this section supports effective governance, strategic alignment, and adherence to regulatory standards. It also facilitates collaboration and communication among various stakeholders, ensuring a cohesive and coordinated approach to AI development and deployment.

AI Use Case Risks

In looking at the **Risks** tab, you may enter Risks and/or you may associate **Compliance Checklist(s)** to be addressed for the Use Case. If you want to use the Compliance Checklist functionality, begin by expanding the **Assign Compliance Checklist(s)** section to see all Active Compliance Checklist(s) and select the checkbox next to the Compliance Checklist(s) you wish to assign questions from.

Click **Next** and you will see the active questions available, you may select the applicable questions to assign.

Details

AI Features

Data Sources

Models

Endpoints

Risks

Stakeholders

More

> Metrics

> Risks

> Compliance Q&A

< Assign Compliance Checklist(s)

The **Active** Compliance Checklist(s) are shown below, please select all that apply to this AI Use Case. Each question will be created as a risk to track the response and allow for further feedback.

Select the Compliance Checklist(s) to Assign to the Use Case

Q Search this list...

2 of 2 items • 0 items selected

☐ AI Compliance Checklist Name	# of Active Questions
☐ 2024 Executive Order 14110	7
☐ 2024 Security Compliance	1

Next

Click **Next**. The selected questions will be assigned to the Use Case as Risks to be addressed. The Questions that had a **Default Decision Maker** assigned will already be assigned, but if no default was assigned, you may take the next step to define. Expand the **Assign Stakeholders to Compliance Checklist Questions** section and associate the Questions on the left with any Stakeholders on the right.

< Assign Stakeholders to Unassigned Compliance Questions

The **Unassigned** questions are presented below. Select the Compliance Checklist Question(s) and the corresponding Stakeholder to assign to below:

Compliance Questions to Assign

2 of 2 items • 0 items selected

☐ Question
☐ If applicable, how is the agency ensuring compliance with Information Quality Act guidelines?
☐ Has the Senior Agency Official for Privacy (SAOP) assessed the privacy risks associated with this AI use case?

Available Stakeholders to Assign

2 of 2 items • 0 items selected

☐ Stakeholder Name	Role
☐ Jen	
☐ Jakub	

Note: Click the **Stakeholders** tab and add any Stakeholders, that have not been associated to the use case.

AI APPLICATION IMPLEMENTATION

The AI Application Implementation section is designed to manage and document the implementation of AI applications that

incorporate multiple AI Use Cases. Each implementation can encompass several AI Use Cases, providing a unified view of how various AI functionalities are brought together within a single application. This setup facilitates the management of complex AI systems, ensuring that all components are effectively integrated and aligned with the application's overall goals.

Technical Notes

FLOWS

Name	Description	Input
AI Use Case Active Compliance Checklist Selection	Allows a user to select the active Compliance Checklist Questions from Active Compliance Checklists to associated to a specific AI Use Case.	recordId from AI Use Case
AI Use Case Compliance Checklist Question Stakeholder Assignment	Allows a user to associate Stakeholders from an AI Use Case to Compliance Questions that have not been assigned a Decision Maker.	recordId from AI Use Case
Auto Assign Compliance Checklist Questions	Called from the AI Use Case Active Compliance Checklist Selection flow to assign the user selected Compliance Questions to the AI Use Case. This may be run stand alone to assign all Active Compliance Checklist Questions from Active Compliance Checklists.	recordId from AI Use Case
aig Clone Use Case	Used to clone an AI Use Case, leveraging various subflows to copy the associated detail records.	recordId from AI Use Case
aig Create Test Case from Risk	Used to create a Test Case from a Risk	recordId from AI Use Case
AIG Sub Flow Clone AI Features	Used by the aig Clone Use Case flow to clone AI Use Case Features.	
AIG Sub Flow Clone Endpoints	Used by the aig Clone Use Case flow to clone AI Use Case Endpoints.	
AIG Sub Flow Clone Models	Used by the aig Clone Use Case flow to clone AI Use Case Models.	
AIG Sub Flow Clone Risks	Used by the aig Clone Use Case flow to clone AI Use Case Risks.	
AIG Sub Flow Clone Stakeholders	Used by the aig Clone Use Case flow to clone AI Use Case Stakeholders.	
AIG Sub Flow Clone Data Sources	Used by the aig Clone Use Case flow to clone AI Use Case Data Sources.	

LWCS

Name	Description	Available for
aigRiskMatrix	Generates a graphical risk matrix based on the Impact and Likelihood scores for a particular risk.	AI Use Case Risk page
aigMultipleChoicePLGen	Renders the corresponding question from the Compliance Checklist Question with the appropriate Response Type (either a picklist field using the possible options in Compliance Checklist Question Response Choices or a text field).	AI Use Case Risk page