

UST Prism – Service Definition



U -
S T

ust.com

Copyright and Confidentiality

Copyright © 2024 by UST Global Inc. All rights reserved. This document is protected under the copyright laws of United States, India, and other countries as an unpublished work and contains information that shall not be reproduced, published, used in the preparation of derivative works, and/or distributed, in whole or in part, by the recipient for any purpose other than to evaluate this document. Further, all information contained herein is proprietary and confidential to UST Global Inc and may not be disclosed to any third party. Exceptions to this notice are permitted only with the express, written permission of UST Global Inc.

UST® is a registered service mark of UST Global Inc

UST

5 Polaris Way,
Aliso Viejo,
California 92656
United States

Table of Contents

A. SERVICE DEFINITION 4

FEATURES: 4

B. ROLES AND RESPONSIBILITIES 6

A. Service Definition

Supplier will provision the **UST Prism** Software for the Customer in the Customer's environment. The Supplier will be responsible for the installation, support and maintenance of the Software during the term of the engagement. The Software shall be accessed or used by the users from Customer's organisation strictly in accordance with terms mentioned.

The Software is an enterprise AI governance platform designed to enable organizations to assess, monitor, and manage AI-related risks across their entire AI portfolio in compliance with global regulatory frameworks including EU AI Act, NIST AI RMF, and ISO 42001.

As part of the engagement, Supplier will stand-up a Sprint team to collaborate and build governance workflows and custom integrations identified by the Customer. The terms of billing and usage is outlined in the Pricing and Schedule document.

Supplier will adopt SCRUM/Sprint based delivery methodology for development and will own the delivery of the work packets. Based on agreed intervals, Customer will be involved to discuss and review the progress.

As part of the initial deployment, the Supplier will work with the Customer teams (including legal, compliance, and security) to ensure that the platform configuration, risk frameworks, and control mechanisms align with the Customer's organizational policies and regulatory requirements.

Features:

The Software comes with the following set of features, which will be deployed for the Customer:

Core AI Governance Layer:

Multi-Framework Risk Assessment Generate comprehensive risk assessments for AI services based on service tier classification (High, Limited, Minimal risk) aligned with EU AI Act, NIST AI RMF, and ISO 42001 frameworks. The platform evaluates 104 pre-configured AI service types across 13 categories including customer-facing systems, financial services, healthcare, manufacturing, and enterprise operations.

AI Register Management Create and maintain centralized inventories of all AI systems deployed across the organization. Each register entry captures the AI service, associated regulatory framework, generated risk assessments, mitigation strategies, and compliance status.

Risk Categorization Automatically categorize identified risks across seven dimensions: Technical, Operational, Ethical, Legal, Social, Environmental, and Geopolitical. Each risk is assigned likelihood and impact scores with automated risk level calculation (Critical, High, Medium, Low).

Secure Access The platform is integrated with customers' identity providers (Active Directory, SSO) and ensures role-based access control for each service within the Software. Multi-factor authentication (MFA) is supported for administrative functions.

Auditing The platform maintains comprehensive audit logs of all user actions, risk assessments, control modifications, and attestation activities. Audit trails are exportable and retained based on customer-defined policies.

Risk Control Management Layer:

Multi-Type Control Framework Define and monitor four types of mitigation controls:

- **API Metric Controls:** Automated monitoring of external metrics endpoints with configurable thresholds (e.g., model accuracy, fairness scores, performance indicators)
- **Document Controls:** Track required documentation with review schedules and compliance deadlines (e.g., model cards, data specifications, impact assessments)
- **Attestation Controls:** Periodic manual certifications with frequency-based scheduling (daily, weekly, monthly, quarterly, annual)
- **Checklist Controls:** Task-based validation workflows with completion tracking

Real-Time Status Monitoring Control status is automatically calculated based on configuration: API metrics evaluate threshold compliance, document controls track review deadlines, attestations monitor due dates, and checklists calculate completion percentages. Status indicators (OK, Warning, Fail, Pending) provide instant visibility.

Governance Dashboard Centralized view of all AI services, associated risks, and control status aggregation. Executives and governance teams can monitor overall compliance posture, identify risks requiring attention, and track control effectiveness across the entire AI portfolio.

Analytics and Reporting Layer:

Data Export and Portability Full data export capabilities in multiple formats (JSON, CSV, Excel, SQLite database) with no proprietary lock-in. All AI registers, risk assessments, control configurations, and audit histories are exportable via self-service interface or RESTful API.

Compliance Reporting Generate professional Excel and PDF reports for regulatory submissions, internal audits, and stakeholder communications. Reports include service inventories, risk matrices, control status summaries, and attestation histories.

Analytics Dashboard Track platform usage, control status trends, and governance metrics. Monitor the distribution of risk levels across the AI portfolio and identify areas requiring governance attention.

Integration and Customization:

API Access RESTful API enables integration with existing enterprise systems including IT service management, GRC platforms, and monitoring tools. API documentation provided in OpenAPI (Swagger) format with sandbox environment for testing.

Custom Configuration Tailor risk frameworks, control templates, and assessment workflows to organization-specific requirements. Platform supports custom risk categories, mitigation strategies, and framework requirements.

Multi-Cloud Support Platform-agnostic deployment on public, private, hybrid, or community cloud environments. Compatible with Azure, AWS, Google Cloud, and on-premises infrastructure.

B. Roles and Responsibilities

Customer	Supplier
System Specific:	System Specific:
Manage cloud subscription and infrastructure provisioning (if applicable)	Manage and oversee the deployment and operation of UST Prism Software
Provide access to Customer's cloud subscription (Azure/AWS/Google) with required authorisations if cloud deployment is selected	Provide technical specifications for required compute resources, networking, and storage
Platform Specific:	Platform Specific:

Customer	Supplier
Define organizational AI governance policies, risk tolerance levels, and control frameworks	Configure platform according to Customer's governance requirements and regulatory obligations
Establish internal AI Governance Committee to oversee platform usage, define risk acceptance criteria, and approve control frameworks	Provide platform administration training and best practice guidance for AI governance workflows
Continuously monitor control status through governance dashboards to identify risks and compliance gaps	Maintain periodic software updates, security patches, and feature enhancements to improve platform capabilities
Assign risk owners and control owners for each AI service in the register	Provide technical support for control configuration, API integrations, and metric monitoring
Conduct regular attestations and complete assigned checklists per defined schedules	Supply documentation for control types, status calculation logic, and integration capabilities
Provide feedback on platform functionality, report issues, and suggest improvements for governance workflows	Provide dedicated support for troubleshooting, user enquiries, and platform optimization
Review and approve risk assessments generated by the platform, customizing as needed for organizational context	Ensure platform availability per agreed SLAs and provide incident response for service disruptions
Maintain API endpoints for automated metric controls and ensure connectivity for monitoring integrations	Validate API connectivity, assist with endpoint configuration, and troubleshoot integration issues
Periodically review audit logs and export data for regulatory reporting and internal compliance reviews	Provision audit logging features, ensure data export functionality, and maintain

Customer	Supplier
	data retention capabilities per Customer requirements

U .
S T

Together,
we build for
boundless
impact