VALIDMIND®

THE AI GOVERNANCE PLATFORM

Public APIs and Integrations

Introduction

ValidMind provides public APIs and libraries that allow organizations to embed the platform directly into their existing workflows and enterprise systems. These capabilities are central to ValidMind's design, ensuring flexibility, extensibility, and ease of adoption across diverse IT environments. Whether deployed as SaaS, in a ValidMind-managed virtual private cloud (VPC), or in a client-managed VPC (on-prem), all deployment models provide the same API and integration features.

This whitepaper provides an overview of ValidMind's integration capabilities, methods, and practical use cases for organizations looking to incorporate AI governance into their existing technology ecosystems.

Overview of Public APIs

ValidMind's Public REST API is secure, JSON-based, and designed to scale with enterprise needs. It provides programmatic access to the platform's core entities, enabling clients to manage model metadata and organizational context without manual intervention.

Through the API, clients can:

- **Manage Model Inventory:** Register models, update metadata, and retrieve model details programmatically.
- **Organize Models:** Secure models into groups, business units and use cases.
- **Manage Custom Fields:** Create, update, and retrieve custom field values for models and artifacts.
- **Handle Artifacts:** Log and manage model artifacts with full lifecycle support.
- **Manage Stakeholders:** Add and update model stakeholders and ownership assignments.
- **Define Relationships:** Create upstream and downstream model dependencies.
- **Retrieve Templates:** Access template definitions to support standardized documentation.
- **Retrieve Analytics Data:** Extracts model status and analytics for reporting and dashboards.
- **Trigger Workflows:** Start or resume workflow executions via webhook endpoints.

API access requires an API key and secret, obtained from the ValidMind Platform. All requests are encrypted via HTTPS, and role-based permissions determine which endpoints a client can use. This ensures that API use is secure and consistent with the user's role in the platform. Interactive API documentation is available via Swagger at the platform's API endpoint, providing detailed specifications for all available endpoints.

While the API provides robust access to model inventory and organizational data, tasks such as executing validation tests and generating documentation are handled through the ValidMind Library rather than the Public REST API.

Integration Categories

ValidMind supports integrations across several categories that align with enterprise workflows:

Model Development and Data Science Tools
The ValidMind Libraries for Python, SAS and R integrate directly into modern model development environments. Data scientists can use the library to register models, capture metadata, and run built-in tests without leaving their environment. The ValidMind Library is natively compatible with popular model development frameworks such as scikit-learn, XGBoost, TensorFlow, PyTorch, and others. The Library also offers customers the ability to extend compatibility to other development frameworks, such as internally developed development libraries.

ML Registry and Model Catalog Integrations
ValidMind connects directly to enterprise ML registries to synchronize model metadata automatically with catalogs such as AWS SageMaker, AWS Bedrock, MLFlow/Databricks, and GitLab. These integrations ensure that model governance data stays synchronized with the source of truth for model development and deployment.

Data and Cloud Platforms
ValidMind's API can be used to enable connection with data platforms such as Snowflake and Apache Spark, enabling clients to link datasets and maintain lineage between raw data and processed datasets. This integration would ensure that the data used in model validation and documentation is consistent with enterprise data sources.

Governance, Risk, and Compliance (GRC) Processes
ValidMind provides its own governance features, including audit trails and compliance reporting. In addition, ValidMind's API can connect with third-party GRC platforms, such Archer and ServiceNow, so clients may integrate outputs generated by ValidMind into their existing governance systems.

Collaboration and Documentation
The platform supports exporting documentation to industry standard formats (e.g., Word), making it easy to share across enterprise documentation tools. Analytics data can be exported to a data warehouse like Microsoft PowerBI, Snowflake, Looker, or Object Storage (Amazon S3, Google Cloud Storage) for custom reporting pipelines.

Integration Methods

ValidMind offers multiple methods to integrate with external systems:

- **Direct API Calls:** Programmatic access to manage models, metadata, and templates.
- **ValidMind Library (SDK):** A Python library that enables developers to log datasets, run tests, and generate documentation within their coding environment.
- **Webhook Events:** ValidMind workflows can be triggered by webhooks from other systems, enabling event-driven automation:
  - Incoming Webhooks: Start new workflow executions when external conditions are met or resume paused workflows from specific webhook steps.
  - Outgoing Webhooks: HTTP Request workflow steps can call external APIs and push data to custom endpoints with secure credential management.
- **Pre-Built Connectors:** Support for direct integration with:
  - ML Registries: SageMaker, Bedrock, MLFlow, GitLab
  - Ticketing and Workflow Systems: Jira, ServiceNow
  - Analytics Platforms: PowerBI, Snowflake, Object Storage
- **Custom Integrations:** Clients can extend integrations using the Public API, library, webhooks, and ValidMind Reference API specification. The platform supports a generic integration framework for connecting to any external system that implements the ValidMind Reference API schema.

Integration Methods Comparison

Method	Description	Client Value	Best Use Cases
Direct API Calls	REST endpoints for managing models, groups, use cases, and templates.	Automates model inventory and metadata management.	Synchronizing models and metadata with enterprise systems and bulk operations.
ValidMind Library (SDK)	Python and R library to run tests, capture metadata, and generate documentation, with ability to run custom developed tests or those from other platforms (Spark, Snowflake).	Embeds ValidMind into model development without leaving coding environments.	Data scientists validating models in Jupyter, RStudio, or CI/CD pipelines.
Pre-Built Connectors	Native connectors for ML registries, data platforms, and ticketing and workflow systems.	Ensures consistency between enterprise systems and model governance.	Automated metadata syncs to maintain lineage in enterprise data environments.
Webhook Events	Incoming and Outgoing HTTPs Webhook events.	Event-driven workflow integration.	Start or resume a workflow in ValidMind from another system when a condition is met; push notifications to external systems.
Custom Integrations	Client-specific integrations built on APIs, library and Reference API spec.	Tailored to unique workflows and systems.	Integrating ValidMind outputs into CI/CD pipelines, custom dashboards, or GRC tools.

Client Use Case: Inventory Field Integration with External ML Registry

Scenario: A financial institution uses AWS SageMaker as their ML platform and needs to maintain synchronized model metadata between SageMaker and ValidMind for governance purposes.

Challenge: The model risk management team requires comprehensive model metadata for governance reviews, but this information is fragmented across the data science team's SageMaker registry and the governance team's ValidMind inventory. Manual data entry is error-prone and creates version control issues.

Solution: Using ValidMind's SageMaker integration, the organization creates a seamless connection between their ML registry and governance platform.

Implementation Steps:

1. Configure the Connection
    - Navigate to Settings → Integrations → Connections
    - Select AWS SageMaker as the Integration Type
    - Provide AWS credentials (Access Key ID and Secret Access Key stored as encrypted secrets)
    - Specify the AWS region

2. Create Model Bindings
    - Link ValidMind inventory models to their corresponding SageMaker models
    - Map external fields to ValidMind custom fields:
        - SageMaker model version → ValidMind "Current Version" field
        - SageMaker deployment stage → ValidMind "Deployment Status" field
        - SageMaker model ARN → ValidMind "External ID" field
        - SageMaker tags → ValidMind "Model Tags" field

3. Enable Automatic Synchronization
    - Configure sync frequency
    - Integration data automatically populates ValidMind fields
    - Manual sync available for on-demand refresh

Business Outcomes:

- **Reduced Manual Entry**: Model metadata flows automatically from development to governance
- **Improved Accuracy**: Single source of truth eliminates version discrepancies
- **Faster Reviews**: Validators have immediate access to current model information
- **Audit Trail**: All sync operations are logged for compliance reporting

Integration Fields Available in ValidMind:

Once synchronized, the following fields become available throughout the platform:

- External model ID, name, and version
- Deployment stage and status
- Model tags and metadata
- Last sync timestamp
- External URL for direct navigation to SageMaker

These fields can be used in:

- Workflow routing (e.g., require additional approval for production deployments)
- Analytics dashboards (e.g., models by deployment stage)
- Automated notifications (e.g., alert when model version changes)
- Compliance reporting (e.g., audit trail of model lifecycle)

Client Use Case: Workflow Integration via Webhooks

Scenario: A bank's model validation team uses ServiceNow for incident management and needs to automatically create incidents when ValidMind detects data drift or model performance degradation, and resume validation workflows when incidents are resolved.

Challenge: The current process requires manual coordination between the model monitoring team (using ValidMind) and the IT operations team (using ServiceNow). When performance issues are detected, someone must manually create a ServiceNow ticket, and when the ticket is resolved, someone must manually update ValidMind to continue the review process.

Solution: Using ValidMind's webhook capabilities, the organization creates bidirectional integration between ValidMind workflows and ServiceNow.

Implementation Steps:

Part A: Outgoing Webhook (ValidMind → ServiceNow)

1. Create a Webhook Secret
    - Navigate to Settings → Integrations → Secrets → Webhook Secrets
    - Add a secret for ServiceNow authentication (Basic Auth or API Token)
2. Configure Workflow HTTP Request Step
    - Add an HTTP Request step to the monitoring workflow configuration in ValidMind
    - Configure the POST request to ServiceNow's incident API
    - Add authentication header
3. Add Webhook Wait Step
    - After the HTTP Request, add a Webhook step configured to wait
    - Copy the unique webhook URL for the workflow step
    - Configure the step to pause workflow execution until webhook is received

Part B: Incoming Webhook (ServiceNow → ValidMind)

1. Configure ServiceNow Business Rule
    - Create a business rule in ServiceNow triggered when incident state changes to "Resolved"
    - Configure the rule to POST to ValidMind's webhook URL
2. Workflow Resumes Automatically
    - When ServiceNow sends the webhook, ValidMind receives the signal
    - The paused workflow resumes from the webhook step
    - Subsequent steps (e.g., re-run validation tests, update workflow status) execute automatically

Business Outcomes:

- **Automated Incident Creation:** Performance alerts automatically generate ServiceNow tickets
- **Seamless Handoff:** IT operations receive complete context without manual data transfer
- **Automated Workflow Resumption:** Resolved incidents automatically trigger continued validation
- **Complete Audit Trail:** Both systems maintain synchronized records of the incident lifecycle
- **Reduced Cycle Time:** Eliminates manual coordination delays between teams

Webhook Capabilities Summary:

Direction	Trigger	Action	Authentication
Outgoing	Workflow step execution	HTTP POST to external system	Webhook secrets (encrypted)
Incoming	External system event	Start or resume ValidMind workflow	API key + secret headers

Why Choosing the Right Integration Method Matters

Choosing the proper integration method ensures that ValidMind aligns with your organization's workflows, technology strategy, and resource availability.

- **Speed vs. Customization:** Pre-built connectors and the ValidMind Library offer fast adoption with minimal configuration, while direct API calls and custom integrations provide greater flexibility for unique requirements.
- **Resource Alignment:** Ensures IT, data science, and risk management teams can adopt ValidMind without overextending resources. Pre-built connectors require minimal technical effort, while custom integrations can be developed incrementally.
- **Strategic Fit:** Supports priorities ranging from embedding model validation in CI/CD pipelines to integrating outputs into compliance reporting.

By aligning integration choices with organizational goals, clients maximize ValidMind's efficiency and impact while minimizing friction in adoption.

Security and Compliance

Data Security

All API endpoints are accessed via HTTPS, ensuring encryption in transit. Authentication uses API keys and secrets, with role-based access control enforcing user permissions. API usage is logged for auditability.

Secrets Management

Integration credentials are stored securely with enterprise-grade protection:

- **Encrypted Storage:** All secrets encrypted at rest using industry-standard encryption.
- **Isolated Storage:** Secrets stored in a separate database from primary application data.
- **Write-Only Access:** Secret values cannot be retrieved once set-only overwritten.
- **Lifecycle Management:** Support for expiration dates and manual revocation.
- **Usage Tracking:** Last-used timestamps for security monitoring.

Audit Trail

The ValidMind Platform maintains a complete audit trail of all changes, supporting compliance with regulatory standards in financial services and other industries. Clients can rely on these built-in capabilities to meet strict governance requirements.

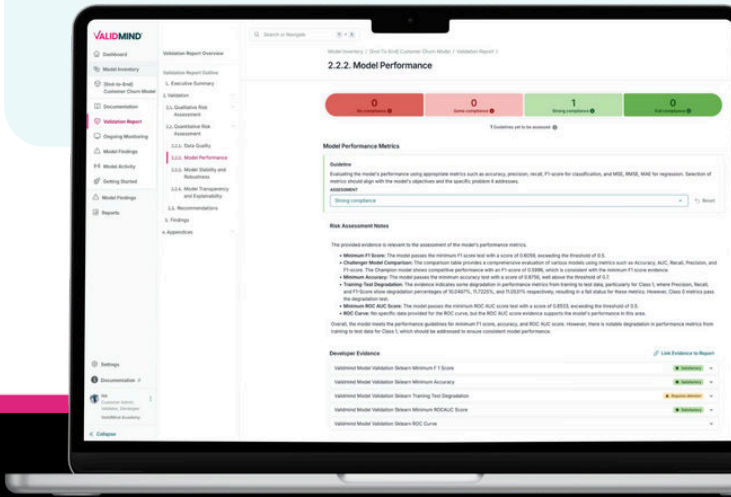
Support and Extensibility

ValidMind maintains detailed API documentation and developer resources. The Public API is versioned and uses deprecation notices to warn users of upcoming API changes. Interactive Swagger documentation provides complete endpoint specifications.

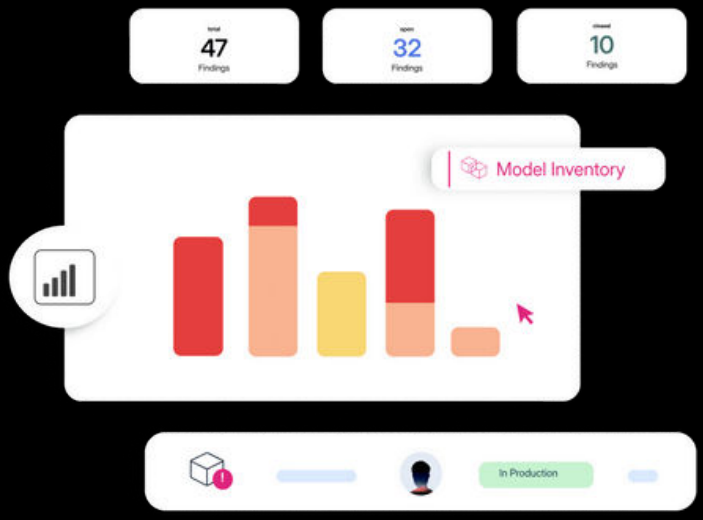
Clients can extend ValidMind's capabilities through:

- **Custom Fields:** Define organization-specific metadata schemas.
- **Custom Integration:** Build connections to any system using the Reference API specification.
- **Workflow Automation:** Design complex approval and notification flows.
- **Library Extensions:** Add custom tests and metrics to the ValidMind library.

ValidMind's solution architects are available to guide clients through complex integration scenarios and custom implementation requirements.



VALIDMIND®



About ValidMind

ValidMind is the enterprise AI governance platform for regulated organizations deploying AI, GenAI, and agentic AI at scale. Built on decades of model risk management (MRM) rigor, ValidMind provides centralized oversight, accelerates AI adoption, and delivers measurable ROI across modern AI systems. By extending proven MRM controls—including independent validation, audit trails, and evidence generation—ValidMind enables banks and financial institutions to scale AI innovation without scaling regulatory or operational risk.

Learn more at www.validmind.com

Conclusion

ValidMind's APIs and integrations ensure the platform fits seamlessly into enterprise workflows. Clients benefit from flexibility, automation, and compliance alignment, reducing operational friction while enhancing transparency and governance.

By providing a Public REST API, a Python/R library, pre-built data connectors, webhook support, and a framework for custom integrations, ValidMind enables organizations to adopt the platform in ways that best suit their environment and regulatory requirements.

Whether synchronizing model metadata from ML registries, automating incident creation in ticketing systems, or building custom governance workflows.