DataRobot

SOLUTION BRIEF

Machine Learning Governance Framework with DataRobot MLOps

The big data revolution means that predictive models are an increasingly integral part of business processes. This creates a growing problem for managing model performance, especially at scale. Often, leaders are lacking visibility into what models are deployed or how they are performing and are unable to confidently assess the risk they pose for the company, their customers, or the bottom line. Aside from this operational problem, enforcement of model regulations is increasing globally, creating an urgent need for transparency and explainability. Without those guardrails in place, there are serious consequences looming ahead.

A robust ML governance framework helps to mitigate the challenges associated with predictive models deployed into production without slowing down your realized business value. With DataRobot MLOps, you can operationalize the ML lifecycle with confidence by using capabilities to monitor, manage, and maintain your workloads. With automated compliance documentation, and audit trails, you don't have to wonder if your models are creating a potential threat and you are prepared to handle an inquiry from regulators.

After the financial crisis of 2008, regulators around the world began to monitor model risk management practices in earnest, starting with the U.S. Federal Reserve Board (FRB) 's SR 11-7. This issue is now trending globally with the EU AI Act[1] released in 2021, and CP6[2] from the Bank of England in June 2022. Regulatory attention and the need for responsible practices to curb model risk in financial markets has only grown with the rapid increase in adoption of machine learning.

The sheer volume of models that financial service institutions are deploying has skyrocketed to optimize performance, taxing teams' operational capacity. A lack of production framework in the ML lifecycle creates clogged pipelines and leaves already overstretched teams with an overwhelming amount of work around maintenance and explainability.

Volume isn't the only concern. Over the last several years, models have gotten increasingly complex with modeling techniques and algorithmic advancements moving beyond traditional linear regression models. And what happens when one model depends on another? More varied datasets that include both structured and unstructured data add to the challenge.

The volume of models and complexity compounds the concern for managing these models and the risks posed and further amplifies the need for proper governance and model risk management. Meanwhile, regulators are quickly catching up and not only enforcing existing regulations, but increasing them to ensure responsible ML governance frameworks, particularly in financial services.

1800% Growth
in the number of bills passed that contain "artificial intelligence" across 25 countries between 2016 and 2021[3]

25% Jump
in the number of models for U.S. banks since 2019[4]

[1]ArtificialIntelligenceAct.eu
[2]Bank of England, Model risk management principles for banks
[3]Stanford, Measuring trends in artificial intelligence
[4]McKinsey & Company, Model risk management 2.0 evolves to address continued uncertainty of risk-related events

Chief risk officers and business leaders need to balance an enormous variety of factors to manage model risk responsibly.

Do they spend more to keep up with model demand or accept higher risk? How do they tackle a shortage of qualified talent for performing model validations? Is it feasible to manage multiple models across different lines of business without a centralized inventory?

The consequences of a poorly developed ML governance framework include job loss, brand or reputational damage, financial setbacks, reduced operating performance, or punishing fines.

Finally, businesses can't ignore the danger of being outpaced by competitors if they fail to keep up with trends in AI modeling.

U.S. $97 million:
An SEC settlement imposed on four Transamerica entities in 2017 for misleading customers[5]

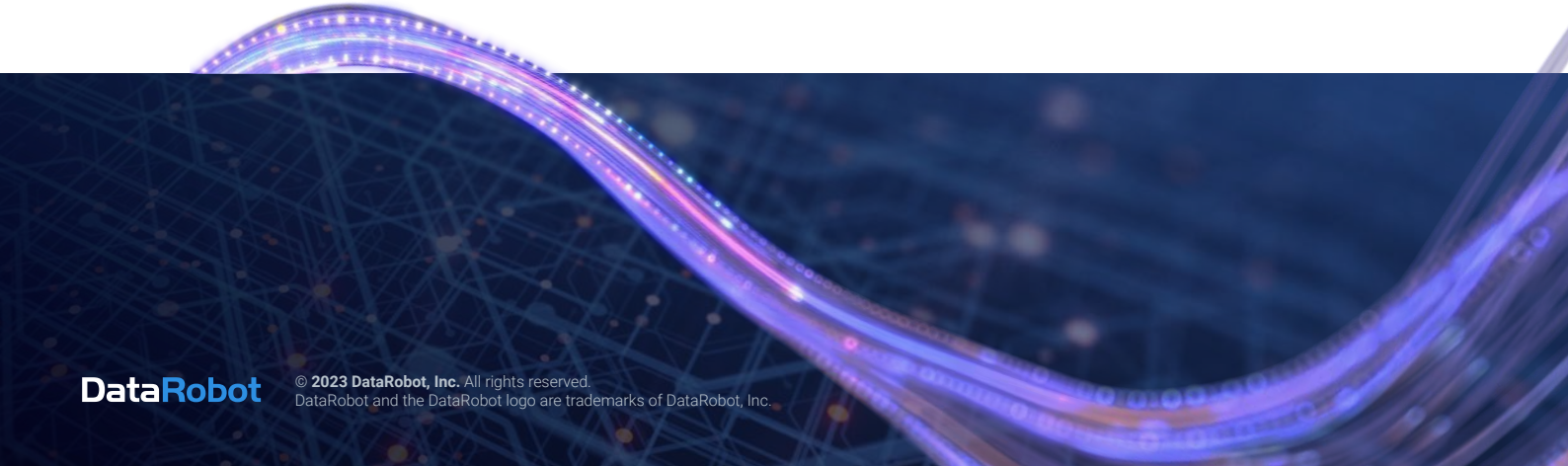
50% of Banks
in a 2021 survey already considered AI or ML capabilities part of their definition of a model.[6]

How well is your business managing model risk?

When you're considering your ML governance framework, ask yourself these questions:

- **How many models can you successfully support?**
- **Do you know who created your models, with what data, when, and for which use case?**
- **Can you ensure the accuracy of your existing models?**
- **How do you uncover and remediate issues?**
- **What's the resource cost for your ML governance framework?**

[5]U.S. Securities and Exchange Commission, Transamerica Entities to Pay $97 Million to Investors Relating to Errors in Quantitative Investment Models
[6]KPMG, Modern strategies for a bold new era of Model Risk Management



DataRobot

What does an effective ML governance framework look like?

ML governance establishes the rules and controls for your machine learning models, including access, testing, validation, logs, and tracking results. With a proper governance framework in place, teams move faster, use ML more often, and manage risk more actively. All of this means that you can scale your machine learning investment and be sure you're aligned with regulatory requirements.

Clear roles and responsibilities ensure that your team members know where they fit into workflows.

Establish clear roles like production model manager or validator within your model lifecycle. Each role description should include duties, qualifications, capabilities, and any training or certification requirements.

Access control helps teams maintain control over production environments.

You should limit access to production data for model training, deployment, modification, or A/B testing, either at the individual user level or through role-based access control (RBAC).

Change and audit logs ensure legal and regulatory compliance.

Knowing when a change occurred and who made it is critical for compliance, as well as troubleshooting when something goes wrong. The system should record actions from both people and software applications or agents.

Records of action support troubleshooting and follow-ups.

For each change to production data, models, or systems, users should provide notes on why they took action that other team members or auditors might find useful. These records can also be beneficial for troubleshooting.

Production testing and validation ensure quality.

To maintain quality, you need to test and validate each new or refreshed model before deployment. Logging these tests and their results demonstrates that models are approved and ready for production.

DataRobot

The model history and version library record model versions as they evolve.

Models will change over time as you update and replace them in production. Maintaining a complete model history, including model artifacts and changelogs, is critical for legal and regulatory compliance.

Traceable model results ensure you meet legal and regulatory obligations.

Building reports for your model results and their deployment status supports both business goals and internal operations. At the same time, it's essential to understand where bias arises in your modeling process.

Data versioning and version tracking provide insights into the lineage of your models.

As your training and production data change over time, a deployed model loses its predictive power. That's known as "data drift." Establish rules around how much data drift is acceptable for your organization's purposes.

Model documentation tracks and presents your results.

Compliance documentation provides evidence that your models work properly, they're appropriate for their intended business purposes, and they're conceptually sound.

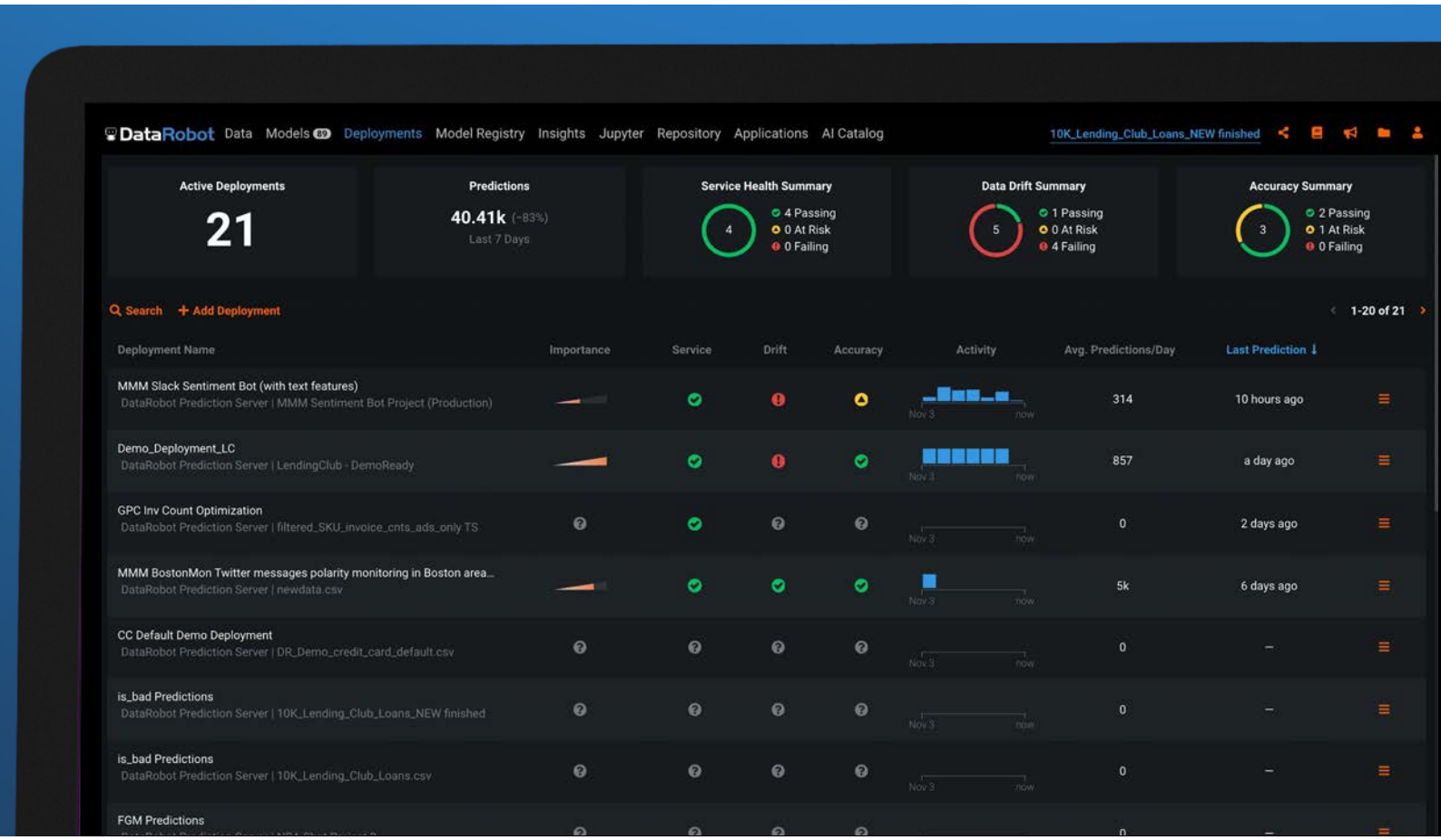
A model inventory houses and manages your models and metadata.

A well-organized and highly navigable model inventory means your people can organize, manage, and access models easily. It supports streamlined assessment, candidate management, continuous evaluation, retraining, and A/B testing.

DataRobot

DataRobot provides a proven ML governance framework through our MLOps platform.

With DataRobot MLOps, IT, infrastructure, and data engineering teams can deploy almost any model to virtually any production environment. As a result, data scientists have the confidence to deploy their models in a well-governed, secure, and compliant environment. Empower your builders to focus on innovation while your IT teams manage compliance, minimize risk, and streamline production.



Ongoing model management and performance monitoring with MLOps

Role-based approval workflows help you define and maintain **clear roles and responsibilities** and maintain **access control**. DataRobot MLOps lets you build approval policies, set up workflows, and simplify change management when personnel turn over.

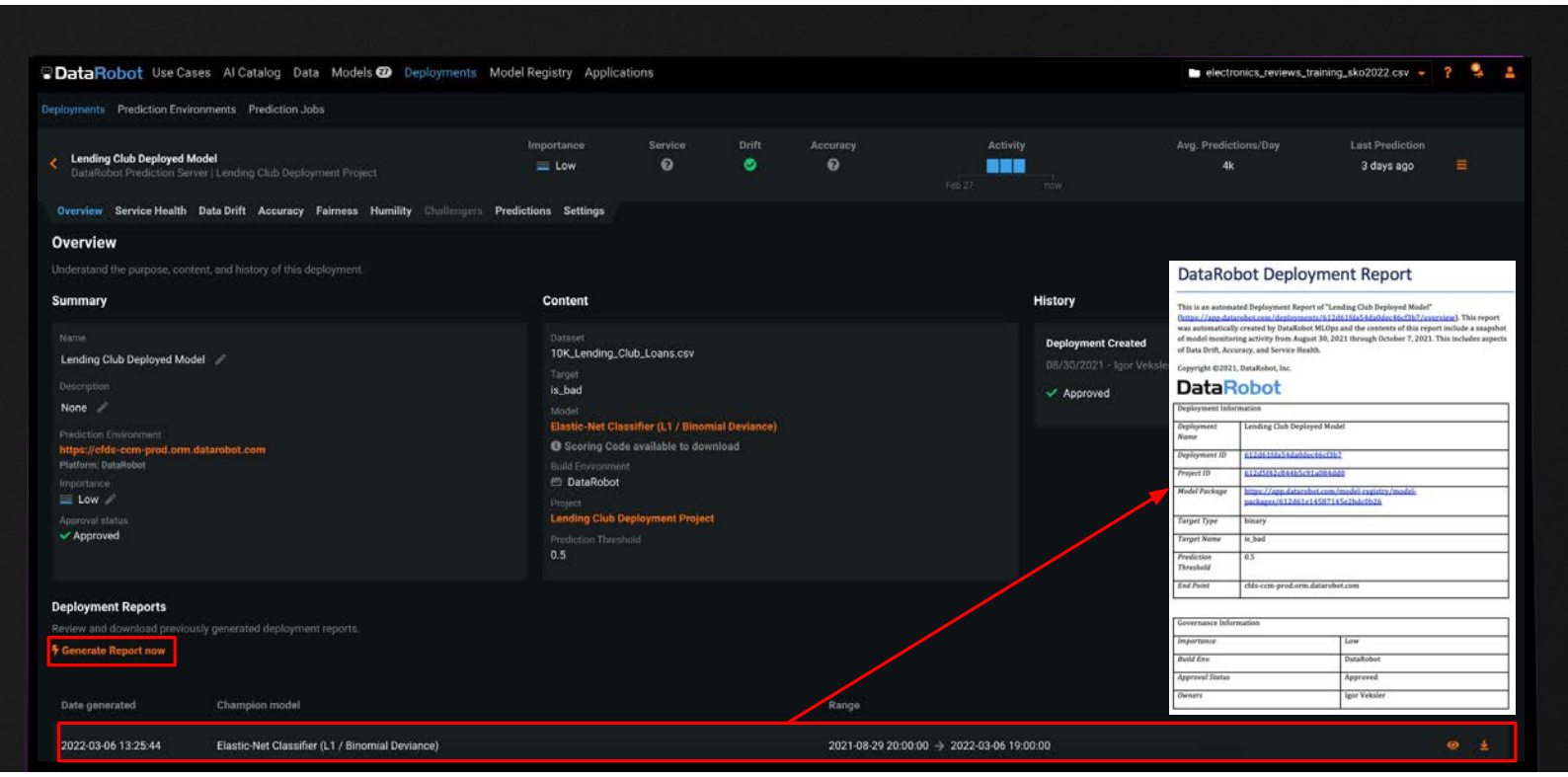
MLOps' integrated **model audit trail** provides traceability through **change and audit logs** and **records of action**. It traces the lifetime of model development, displaying when and where the model was deployed, who made updates, what was changed, with what authority, and why. Meanwhile, integration with messaging systems like Slack or email enables trigger-based notifications.

Benchmark models can be tracked along with production models in MLOps

Integration with CI/CD pipelines automates model testing to accomplish production testing and validation. The DataRobot user model (DRUM) and GUI also provide the ability to test model instantiation, handle missing data, and access model versioning.

MLOps' model registry and documentation features store model artifacts and metadata for all of your organization's models, providing a robust model history and version library. Model validators establish benchmarks using DataRobot's champion/challenger framework to align with alternate second line of defense and first line to test theories.

Templates for customized report building, Model Deployment Reports that cover monitoring activity, and bias and fairness monitoring for protected classes all contribute to highly traceable model results within the MLOps platform.



Automated MLOps Deployment Reports

Humility rules overrule model output based on uncertain data input or output. At the same time, data drift, accuracy, and service health monitoring help you keep an eye on your models' performance in real time, while remote agents automatically monitor models running on an external runtime. Together, these features support thorough data versioning and version tracking.

MLOps provides model documentation for user-built custom models and information on your input datasets. By automating the model development documentation process, we've standardized our content to ensure that it aligns with policy expectations for the documentation of all results.

Custom inference models bring user-generated models onto MLOps' model inventory for monitoring and governance. The platform includes all the models your team has built and their associated metadata.

DataRobot is the leader in enterprise AI, delivering trusted technology and ROI enablement services to global enterprises competing in the Intelligence Revolution.

DataRobot MLOps allows organizations to deploy, manage, monitor, and govern their machine learning models from a single place, empowering different stakeholders to seamlessly collaborate around the common goal of scaling and managing trusted ML models in production.

Our proven combination of cutting-edge software and world-class AI implementation, training, and support services, empowers any financial services organization to drive better business outcomes with AI.

Learn more about DataRobot MLOps at
datarobot.com/platform/mlops

Sign up for personalised demo of DataRobot at
datarobot.com/demo

DataRobot

Contact Us

225 Franklin Street, 13th Floor, Boston, MA 02110, USA

datarobot.com **info@datarobot.com**