

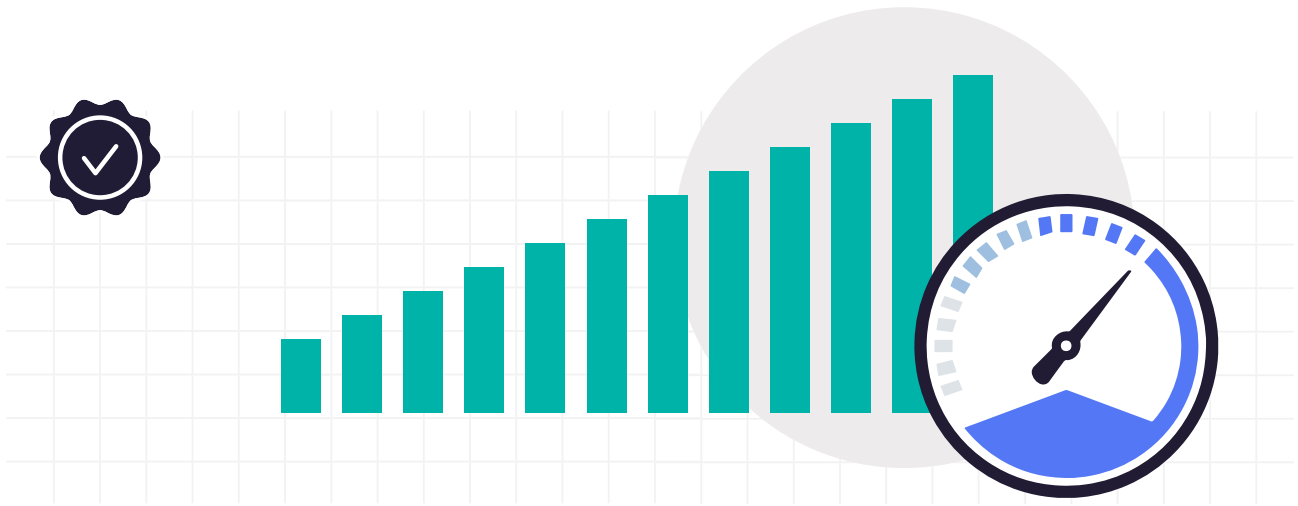
EBOOK

How to Safely Scale AI With Oversight

Operationalizing Analytics & AI Project Governance



The Challenge: Safely Scaling AI at the Speed of the Business



Many companies see the opportunity in AI to radically change the way they do business and accelerate their digital transformation, and organizations have invested despite economic uncertainty during the global health crisis and continued turbulence today. They want to improve customer experience, reduce churn, accelerate innovation, or reduce costs through predictive analytics. In other words, scaled AI affords a real opportunity for impact.

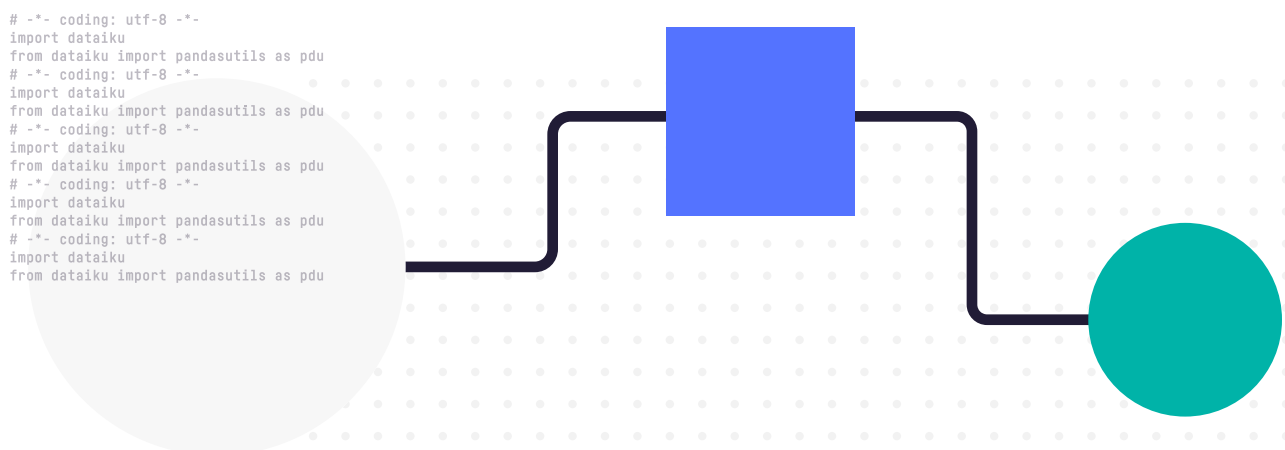
The value at stake is significant. By building machine learning (ML) into processes, leading organizations report process efficiency increases of 30% or more and revenue increases of 5% to 10%.¹ At one healthcare company, a predictive model classifying claims across different risk classes increased the number of claims paid automatically by 30%, decreasing manual effort significantly. In addition, organizations have to develop scalable and resilient processes to not only unlock value for years to come, but ensure they are prepared for any periods of economic change.

However, achieving this AI-enhanced state is not that simple, and companies face challenges. Periods of economic flux, for example, won't just exacerbate these challenges. They may even become too much for companies to face, forcing them to give up and forgo their AI initiatives altogether.

¹ <https://www.mckinsey.com/business-functions/operations/our-insights/operationalizing-machine-learning-in-processes>

In terms of challenges to scaling up with AI, a survey by O'Reilly revealed that only one quarter of respondents described their use of AI as “mature.”² In practice, data and analytics teams waste too much time building and processing ML models. As a result, 90% of ML models never make it into production which, particularly during times where AI budgets are being reduced and costs are being scrutinized, this is a surefire way to get whole budgets or teams cut.³ They also face a significant business value problem that roadblocks investment and leads to the following questions:

- Where is the value in the growing number of AI projects (and models) that a company must manage?
- How do we ensure that we separate the wheat from the chaff, e.g., leverage the right projects that generate value and deprecate the underperforming ones?



Complementary to these business value propositions, companies also face questions about AI risks.⁴ Where AI risk is considered the likelihood of deviation from what is expected or intended across the AI lifecycle, benchmarks may be set internally or externally. Internal policies can be defined by ethical frameworks, business strategy, and defined objectives; externally, new standards and regulatory frameworks are fast-evolving and expected to define new best practices and obligations for AI developers, resellers, and users.

Lack of preparation for conforming to either internal or external requirements means considerable risk exposure which, fully realized, could mean pulling deployments, paying penalties, or facing PR backlash. This ebook will break down helpful strategies and best practices for data and analytics leaders and team managers who wish to safely streamline and scale their AI efforts, whether you are starting your AI journey with a handful of models or actively scaling your use of AI.

2 <https://www.oreilly.com/radar/ai-adoption-in-the-enterprise-2021/>

3 <https://towardsdatascience.com/why-90-percent-of-all-machine-learning-models-never-make-it-into-production-ce7e250d5a4a>

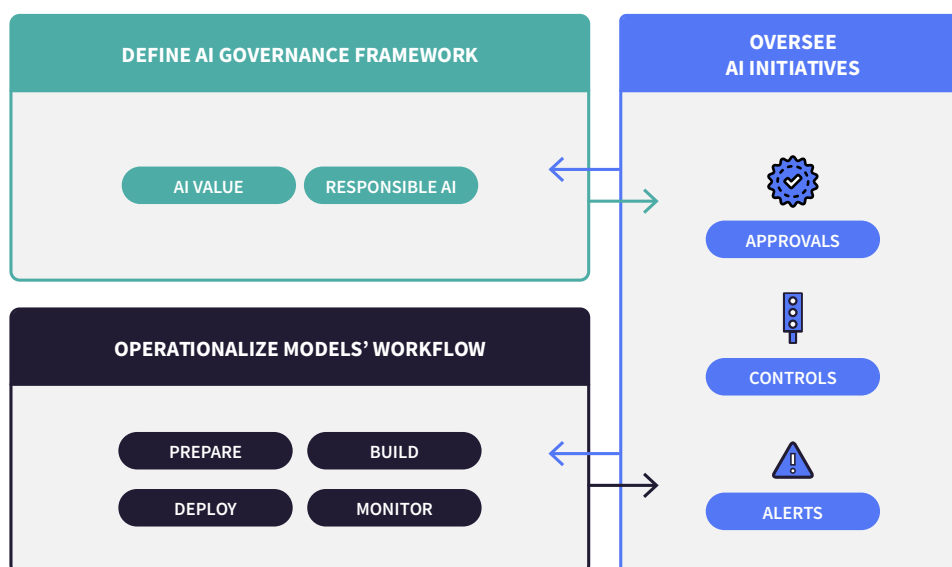
4 <https://www.oreilly.com/radar/ai-adoption-in-the-enterprise-2021/>

Effective Scaling Starts With AI Governance

The only way to scale AI is to build an effective AI Governance program, where “effective” means that individuals building AI projects aren’t encumbered by or worrying about risk themselves, because by definition they’re working in a governed way. By doing so, they will be able to shift their focus to researching and developing efficient models without sacrificing breach of internal or external requirements and concerns about related penalties that are counterproductive to scaling broadly (and use case deployments in particular). A strong AI Governance framework should:

- Centralize, prioritize, and standardize rules, requirements and processes aligned to an organization’s priorities and values
- Inform operations teams, giving build and deployment teams the right parameters to deliver
- Grant oversight to business stakeholders so they can ensure that AI projects (with or without models) conform to requirements set out by the company

Ultimately, because projects are governed, they are controlled, approved, and explained, freeing stakeholders from concerns about risk exposure and the questions-as-impasse, “Can I do this? Did I do this right?” They will now be able to focus on researching and developing efficient models without sacrificing breach of internal or external requirements and concerns about related penalties that are counterproductive to scaling broadly (and use case deployments in particular).



In the next section, we’ll set out to explore how to strike the balance between control and autonomy and get more people involved in AI projects.

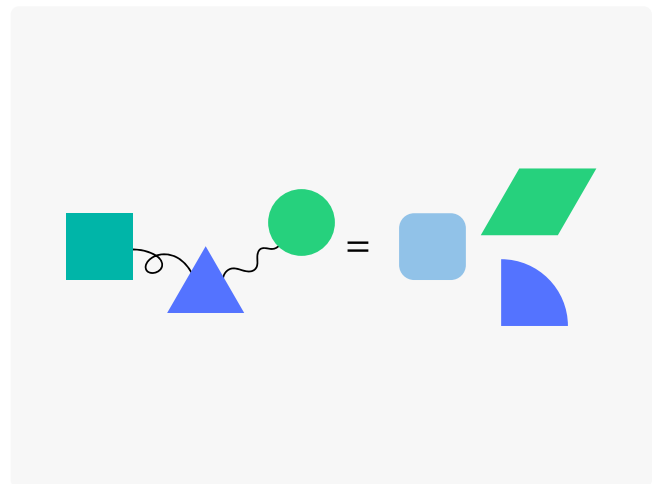
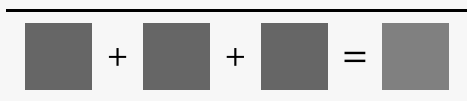
Finding a Modus Operandi: Control and/or Autonomy?

Imagine a scenario where an executive team puts AI scaling into their business strategy. Moving from a couple of models used in one or two business lines, their vision is to expand AI use across business areas, which means building out their data science teams and upskilling their business leads. Their high-level goal is efficiency and growth. And they want to ensure that they use AI effectively and see a strong AI Governance framework and Ops approach as essential.

Concerned with risks posed by AI, they find themselves focusing on prioritizing enforcement of governance rules, requirements, and processes to build confidence that business priorities, regulatory monitoring, and compliance are effective. But, on the road to achieving their strategic objectives and ensuring risk management, they have much to consider:

How much control should we exercise over our teams? How much autonomy should we give them? How centralized or decentralized should our approach be? What are the perks and drawbacks? What should we do?

ON CONTROL: A CENTRALIZED APPROACH



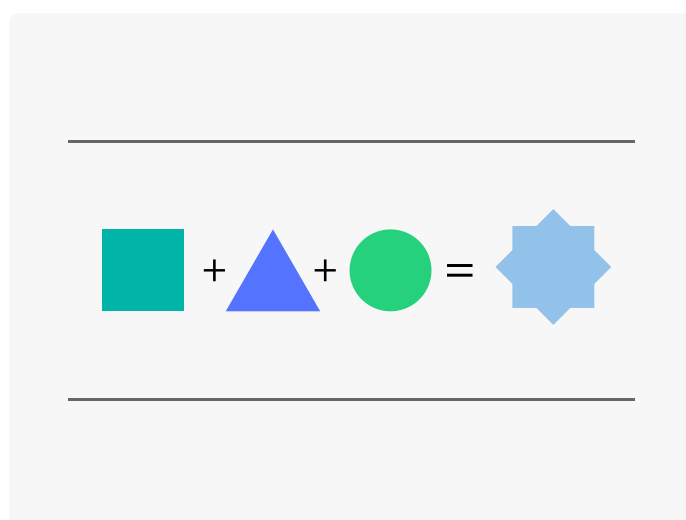
When we think of control at its most extreme, we think of a dynamic where individuals and teams must follow established rules and processes, where the monitoring of rule following is intensive and any overreach is considered out of bounds. Such an extreme might also be viewed as an overly-centralized approach.

ON AUTONOMY: A DECENTRALIZED APPROACH

With respect to autonomy at its most extreme, individuals and teams can do what they like. There are no parameters set in the company and anything goes. We could refer to this approach as being overly decentralized.

Generally,⁵ these extremes are likely to be underproductive: Too much control can stunt innovation and create intensive administrative burdens; too much autonomy, and the potential for risks could increase. So, if not extremes, then what?

BALANCING CONTROL & AUTONOMY: TURN AI INTO A TEAM SPORT WHERE MORE VALUE IS CREATED BY MORE PEOPLE



Let's illustrate this balance with an organization that has successfully overcome information chaos while orchestrating collaboration and involvement: Wikipedia.

What makes Wikipedia different? The knowledge-driven organization delivers governance from the get-go: We can say that they put the users and the authors in the center of their strategy. They established a third role, the curator, who acts as a quality filter for content and who independently assesses content according to established requirements. Wikipedia also brings well-defined rules for data curation, including validation rules and alerts, transparency, and auditability.

⁵ <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-evolution-of-model-risk-management>

This is what makes the model so unique, though: Although Wikipedia has more than 33 million registered users and 118,000 active editors, independent surveys have shown that the quality of information is still very high. Wikipedia wins on scalability — today, there are more than five million articles in Wikipedia across 300 editions, managed by just 1,044 administrators. They have the ability to block and unblock user accounts and IP addresses and perform tasks ranging from editing, protecting and unprotecting pages from editing, deleting pages, and renaming pages.⁶

For your AI models, it's the same scalability challenge. You don't slow down the development of analytics and AI projects with erratic and unapproved interactions. Rather, you:



Encourage contributors to work together on multi-disciplinary teams.



Turn AI into a team sport while creating value around analytics projects.



Establish clear and transparent monitoring rules to facilitate the development of qualified, authenticated, and approved models.

Finding the right, balanced approach for your organization will ensure control of the production workflow without restricting innovation and team autonomy. Now that we have discussed the right approach, it is essential to take the necessary steps to regain control over the proliferation of analytics and AI projects.

⁶ https://en.wikipedia.org/wiki/Wikipedia:List_of_administrators

3 Steps to (Re)Gain the Right Level of Control

Before embarking on the steps below, set a governance framework as a foundation in order to support organizational priorities and values. Then, to avoid chaos and (re)gain control over your analytics and AI projects, while also fostering innovation, follow these steps:

1. In step zero, set a governance framework as a foundation in order to support organizational priorities and values.
2. In the first step, gather all of the elements in one central point to have the big picture: an overview of the model development steps. Then, you will need to select projects to prioritize.
3. In the second step, set up necessary safeguards to control analytics and AI projects and models. To avoid «garbage in, garbage out,» it is indeed essential to prevent poorly documented analytics and AI projects from being freely deployed without oversight.
4. During the third step, keep a constant eye on model and project health. If necessary, this would require a revision of the analytics and AI projects in question.

WHAT IS AN ANALYTICS AND AI PROJECT?

An analytics and AI project is a set of artifacts that typically includes:

- The project description and business justification
- Datasets and preparation steps for data transformation (aka the data pipeline)
- Predictive models (if needed)
- Visual insights/outputs (reports and dashboards)
- AI or web applications created for end users

All of these components will go through development, testing, and production.

STEP 1: CENTRALIZE & PRIORITIZE: HOW TO GET THE AI BIG PICTURE

Centralize

Keeping control over the development of AI models in the enterprise is not an easy task: At scale, business teams might be creating low- and no-code models and analytics teams could be creating 10s to 100s of models on a wide range of business areas. All the while, senior or management stakeholders who are ultimately responsible for deployments are looking for the big picture.

When scale introduces the potential for drastic decentralization and management requires some level of understanding of projects in development and production, it becomes necessary to consolidate projects in one place and provide sufficient information that accommodates those senior stakeholders. You must be able to centralize all projects (regardless of their source) while enabling the right stakeholders to check for integrity across the project lifecycle.

All analytics and AI projects, no matter their stage of development, must be monitored. Nobody wants a model to be widely used if flawed, low-performing, or undocumented (not to mention having to pull the plug on a model if it fails because of drift or because it does not meet established requirements).

Many decision makers complain about losing control over analytics and AI projects. Whether they are business or IT decision makers, they all have legitimate expectations. Some questions arise, such as:

- *Are these all the models?*
- *What exactly do these models do?*
- *Who developed them?*
- *For what purpose?*
- *Are they efficient? Are they performing?*
- *Are they business critical? Are they risky?*
- *Who approved them?*
- *Do they need to be updated or replaced?*

Across geographies, *governments are progressing regulation, non-legislated guidance, and standards* explicitly concerned with governing AI:

- The European Union's proposed AI Act establishes a tiered risk framework linked to new requirements for AI systems that are deemed 'high risk.'
- In the U.S., the National Institute for Standards and Technology is building out a non-mandatory AI Risk Management Framework.
- The Singaporean government is progressing their AI Governance Framework.

Altogether, governments and standards organizations around the world are seeking out the development of best practices around developing and deploying AI. These new best practices will be associated with voluntary standards and, in time, new legal obligations.

The Control Tower Analogy: Managing Your AI Traffic

Airports and air traffic management serves as a useful analogy. Over the decades, air traffic has grown exponentially. This growth is materialized by hundreds of thousands of airplanes that must take off and land every day at a specific time in a defined order to allow passengers or goods to travel.

What would happen if there was no control tower?

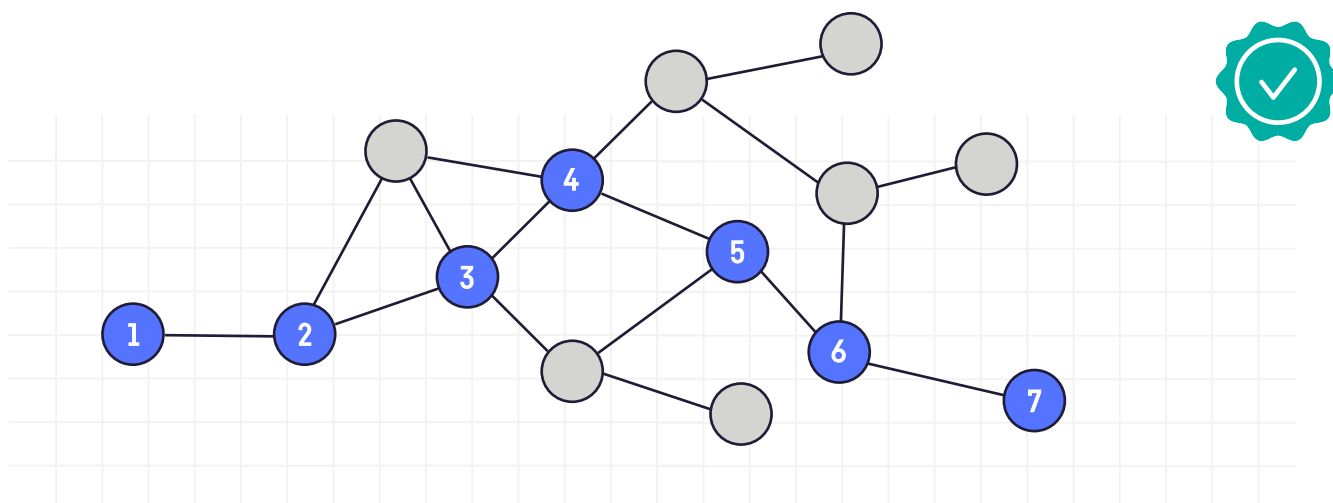
Traffic would be disorganized; passengers would be unhappy. Pilots would land and take off blindly. There would be huge traffic jams and, unfortunately, airplane crashes. This will cause a snowball effect that leads to complete paralysis of air traffic in a whole region.

In this context, what is the role of the control tower? The control tower facilitates traffic flow and guarantees the smooth running of flights safely and effectively. In the control tower, each controller will monitor each aircraft in flight, authorize landings and takeoffs, and ensure that the traffic is regulated according to the rules in place. They will keep the plane's traffic big picture so you can prioritize the ones that matter, so you avoid collisions and allow air traffic to flow smoothly.

That's the same for AI. You need the big picture regardless of model provenance. You will avoid unapproved AI projects moving to deployment AND enable the right ones to deliver value.

Prioritize

Prioritization is vital at this stage. Although all models should be able to be controlled, some might be low risk or sufficiently mundane that they don't require any kind of intervention. Ultimately, you may not need to control all models to the same extent.



Without the ability to prioritize, you may fall back into the failings mentioned in relation to extreme control: potentially stifling innovation by putting the same level of requirements across all models, no matter their purpose. However, you want to keep an eye on what is essential, (i.e., the models ready for deployment, making sure you answer the questions mentioned earlier).

Being able to prioritize enables you to be flexible with your governance process: Adaptive governance becomes a reality here. You can modulate and adapt the level of control you want over both your models and your projects.

Within Dataiku, you can automatically get a view of all your projects and saved models. You can use a dedicated page called “Governable Items” to choose which of these items to “Govern” — meaning identifying which items to manage with the predefined governance plans (to track their status, centralize progress reports, etc.).



Having the means to control does not necessarily mean that you must control everything. As such, it is crucial to preserve the freedom of innovation and the operational capacity of your multidisciplinary data and analytics teams. Once the centralized view and the projects identified and selected are in place, it's time to transition to our second step.

As part of your new operational governance framework, you have designated a person (separate from the project or model team) to approve and validate models. This step is essential to ensure a controlled deployment of the models in production. This designated person also needs a level of power and executive support to turn back projects that are not ready.

This means that model validators and risk managers need a level of power to counterbalance the power of the data science project team. The person in charge of governance will need to have the right indicators of completeness and transparency, validate the checklist before approval, and ensure that it is directly accessible to the approver. The model will then be ready for approval/validation.

Now that we have covered the first step, it is critical to explain and qualify both projects and models.

STEP 2: EXPLAIN AND QUALIFY YOUR ANALYTICS & AI PROJECTS BEFORE PRODUCTION

How can an internal stakeholder or a client trust a project based on an AI model if they don't know why it's being used, how it works, its accuracy (amongst other criteria), or whether the model met all established requirements before deployment?

Transparency of AI projects and associated models is often considered the Achilles' heel of AI. One of the challenges faced by data science teams is being able to answer and explain:

- Why are we doing this? (i.e., Is it a model to satisfy a customer retention objective or reduce the website reader's attention?)
- How does it work?
- How did we arrive at the results?
- Can we challenge the results for confirmation?
- Can we explain the model and its outputs to our senior managers and our customers? (i.e., Does the model meet ethical and transparent model management requirements set in your governance framework?)

TRANSPARENCY IN THE CONTEXT OF AI

Ultimately, different contexts and audiences will require different levels of transparency. This could range, for example, from transparency and explainability around the management of the model to the model's inputs and outputs (and how they were achieved).

Knowing what level of transparency you require is context-specific but, for our purposes, we discuss transparency of management which includes the reason for the project or model, who was involved, what they did, and who signed off for deployment and why.

Actual customers can also have questions that need answers. Let us use the finance sector for example: A customer whose credit request is declined has the right to know why and a bank must provide the reasons. This is why AI systems must produce reason codes for a given score in their outputs.

The description cannot be a random description depending on whoever is filling it. A framework is mandatory so that all your governed projects follow the same description structure and workflow, making them easier to compare on a day-to-day basis while standardizing behaviors and expectations. To achieve this comparison, you need to qualify the projects depending on their risk, value, and feasibility levels.

The notion of risk and value is highly dependent on the company metrics. But once projects are qualified, it will be easy to compare them and keep control of them. Then, you can start engaging key people to keep projects trusted and compliant over time.

Now, here comes the last step: making sure you can deploy AI projects and monitor them closely. You will then let anyone in a company access trusted models in a governed way. At this stage, it is essential to introduce an approval stage directly into the model's lifecycle and make it the center of your operational governance. Without an approval system, you'll end up with chaos in model proliferation.

Dataiku can help you associate extra contextual information to a project, such as specifying the person responsible for a specific project, adding in notes on the latest update on progress, or attaching documentation for a project or a model version.

STEP 3: APPROVING FOR DEPLOYMENT AND MONITORING YOUR MODELS: A KEY INGREDIENT OF YOUR MLOPS STRATEGY

Project deployment is the critical step — the gateway where an analytical insight will be available to internal stakeholders, clients, or even end customers. As such, deployment is a pivotal step to be controlled for governed projects. You must monitor the model in production, check its integrity and, if necessary, choose to deactivate the model if it is underperforming. If you leave faulty, poorly documented, and poorly performing models in production, the consequences can be daunting.

It is why setting up governance rules before deployment is a crucial step. Model signoff will enable the company's risk or governance manager to validate its deployment and invalidate a model that does not meet the pre-defined criteria. It is often the missing link in an MLOps strategy. This step is crucial if you want to deploy your models at scale and avoid any loss of productivity or revenue generation in the long run.

Prevent deployment of projects, bundles (analytics with or without models), and models without a sign-off in Dataiku. The Govern node in Dataiku allows you to require stakeholder review and sign-off on model versions or projects before they are deployed to production.

Focus on the People Behind the Processes

Before controlling, you also need to involve data scientists in the governance system. Otherwise, you risk creating misunderstanding by applying a governance system without putting people at the heart of the process. Do involve the data scientists to define the rules of inclusion or exclusion of models before any deployment. Having approval workflows and sharing them allows the model practitioners to know the workflow and its possible impacts.

After models have been approved for deployment, the monitoring step is essential. The predictive power of AI projects can decay over time as underlying data changes. Without proper monitoring, analytics and AI projects could produce inaccurate predictions which could lead to poor decisions with financial and legal consequences.

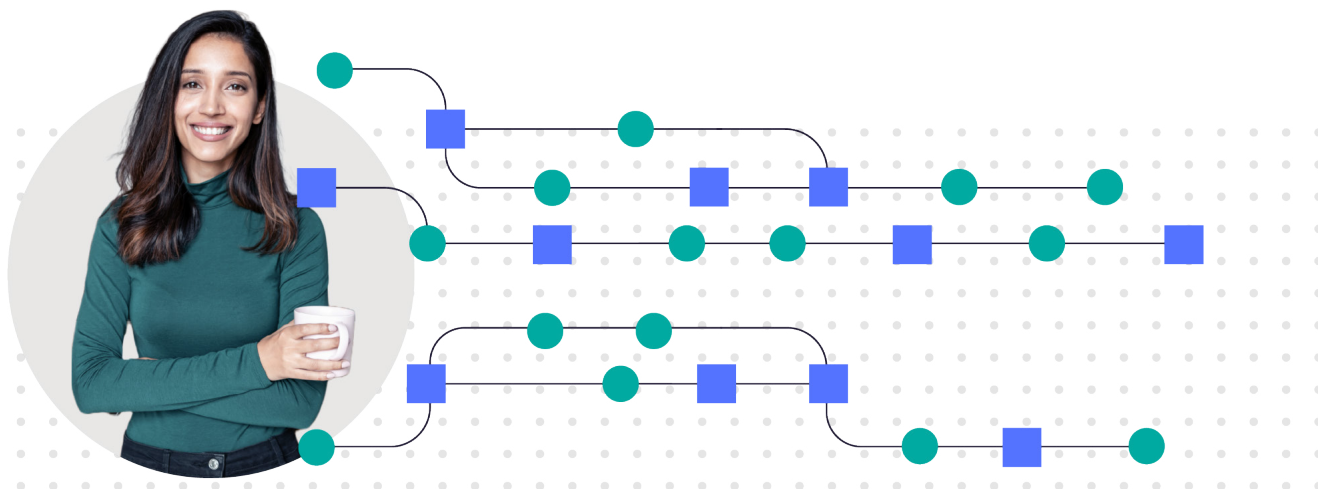
The monitoring answers the following questions:

- How can we detect a degrading model and ensure we have the best performing models in production?
- When is the right time to retrain the model?

It's a real issue that manual operations cannot solve. Monitoring ongoing model performance in production can be time consuming and laborious for data teams. Furthermore, periodic, manual spot-checking is an inadequate solution to detect emerging issues at scale.

Automated checks and monitoring on deployed models alert operators to potential performance. A new model evaluation store provides detailed, historized performance charts and metrics to help inform data scientists and IT operators whether to retrain or refactor a live model. There are many benefits for an automated monitoring approach: First, you will reduce manual oversight. Model evaluations run semi-autonomously, but they will alert operators with early warning of data anomalies or degrading performance. The governance system will automatically record past performance for governance and compliance purposes. In Dataiku, model evaluations alert operators with early warning of data anomalies or degrading performance.

What Is Dataiku Govern? Your Superscale Hero



Dataiku is the platform for Everyday AI, systemizing the use of data for exceptional business results. Organizations that use Dataiku elevate their people (whether technical and working in code or on the business side and low- or no-code) to extraordinary, arming them with the ability to make better day-to-day decisions with data.

As a platform, we have the scope to provide tools to help our customers think about what governing their development and deployment of AI can look like. We also have the scope to build out a form and function that seamlessly ties innovation and exploration to rules, requirements, and processes.

Dataiku Govern enables users to efficiently execute the three stages of scaling that we just listed above, fighting against the barriers and challenges that organizations often face. The capabilities within Dataiku Govern allow users from relevant backgrounds (e.g., project managers, analytics leaders, risk managers, and more) to unlock the value of AI quickly with sustainable control mechanisms, even when facing the pressure to scale quickly.

Dataiku Govern is a dedicated component of Dataiku — it provides a set of features to help organizations structure and control their AI Governance and MLOps processes. These features are meant to work seamlessly with existing Dataiku capabilities. They primarily focus on giving tools for project oversight, risk monitoring, and compliance to analytics leaders and other employees responsible for AI/ML or analytics projects.

At its foundation, Govern provides users with an approach that encompasses critical steps on project and model design, development, and deployment. Dataiku developed Govern capabilities within the platform with diverse organizations in mind. To accommodate that diversity, users are empowered to leverage both predefined and custom workflows to help track their project and model status, adding notes, assignments, and other relevant documentation.

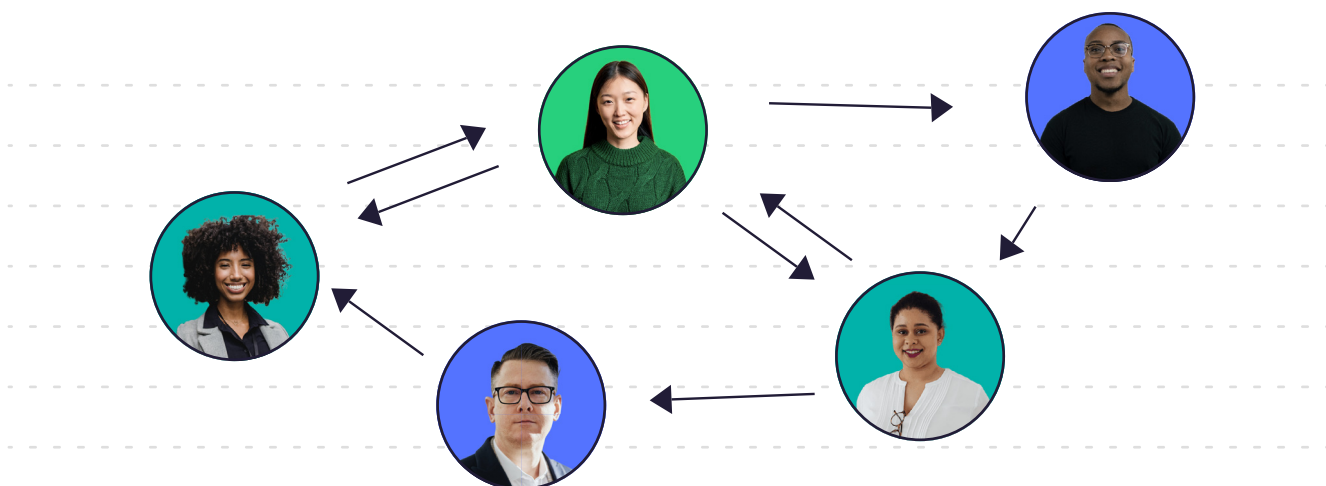
Govern provides them with a model registry, a central repository to review status and performance metrics of all models across projects and Dataiku instances within an organization. Govern also enables coherent project qualification aligned to business priorities: Dataiku provides assessment capabilities on risk, value, and feasibility to help project managers qualify and prioritize projects, with graphs to compare projects to each other.

With model approvals and sign-off, companies can now require specific people to sign off on models before they go to production, with model deployment blocked by Dataiku until proper sign-offs have been given. Company admins can configure which person or role needs to give these approvals based on the project.

Conclusion

Do not underestimate the need for collaboration, especially when dealing with governance. A control layer based on a collaborative platform is vital. Before controlling, though, you need to involve data scientists in the governance system. Otherwise, you risk creating misunderstanding by applying a governance system without putting people at the heart of the process. Do involve the data scientists to define the rules of inclusion or exclusion of models before any deployment. Having approval workflows and sharing them allows the model practitioners to know the workflow and its possible impacts.

Of course, when deploying a model, the control layer alone for the risk and compliance profiles is not enough. By turning AI into a team sport on a single platform (like Dataiku), you'll help everyone — data analysts, IT, ML engineers, data scientists, and risk and compliance teams — with powerful tools and capabilities to operationalize the models.



Indeed, model deployment is no longer the exclusive task of data scientists. It now requires the involvement of the risk and compliance experts. They must work together and the underlying platform must have capabilities that enable collaboration and the right balance between control and autonomy.

Having a complementary view on the same data also allows to de-silo the work and build the necessary trust between teams working in relay on the operationalization of models. This complementarity between the capabilities available for different types of profiles makes the difference.

This ebook highlighted how critical analytics and AI project governance is becoming. Letting models propagate without control will make teams inefficient. While desperately trying to control models, data and analytics practitioners won't have time to focus on innovation or explore new use cases.

At the same time, controlling analytics and AI projects allows the company to set up rules of transparency, usage, access, and trust around AI. There is no time to waste, and the longer you wait, the more you run the risk of letting use cases slip away. No matter how many analytics and AI projects you want to deliver, developing an operational governance is the right thing to do.

Not only does the company protect itself from any future regulatory risk, but it also strengthens its ethical standards. Good governance will foster a proactive attitude towards AI deployment, reinforcing a positive brand perception — an advantage to which all the most dynamic and AI-driven companies aspire.

About the Authors



David Talaga

David Talaga is a Product Marketing Director at Dataiku. David has rich and diverse marketing experience, including strategic, field, and product marketing roles in leading data and AI organizations. After graduating from the EDHEC Business School, David started his career as a data analyst in the healthcare industry.

In 2000, he joined Dassault Systèmes where he held several senior positions, notably heading up the technology partnership program and the strategic alliance with Microsoft. In 2006, David joined Microsoft as Product Marketer for Visual Studio. In 2014, he became Marketing Manager for a new edtech platform at John Wiley and Sons before joining Talend as Product Marketing Director for data quality and data governance. At Dataiku, David focuses on MLOps and AI Governance.



Jacob Beswick

Jacob is the Director of AI Governance Solutions at Dataiku. With a background in AI regulation and governance within the U.K. government's Office for AI, Jacob is responsible for thought leadership on AI Governance, which includes getting involved in the evolving regulatory and standards landscape and working to put emerging guidelines and requirements into practice in Dataiku's platform.

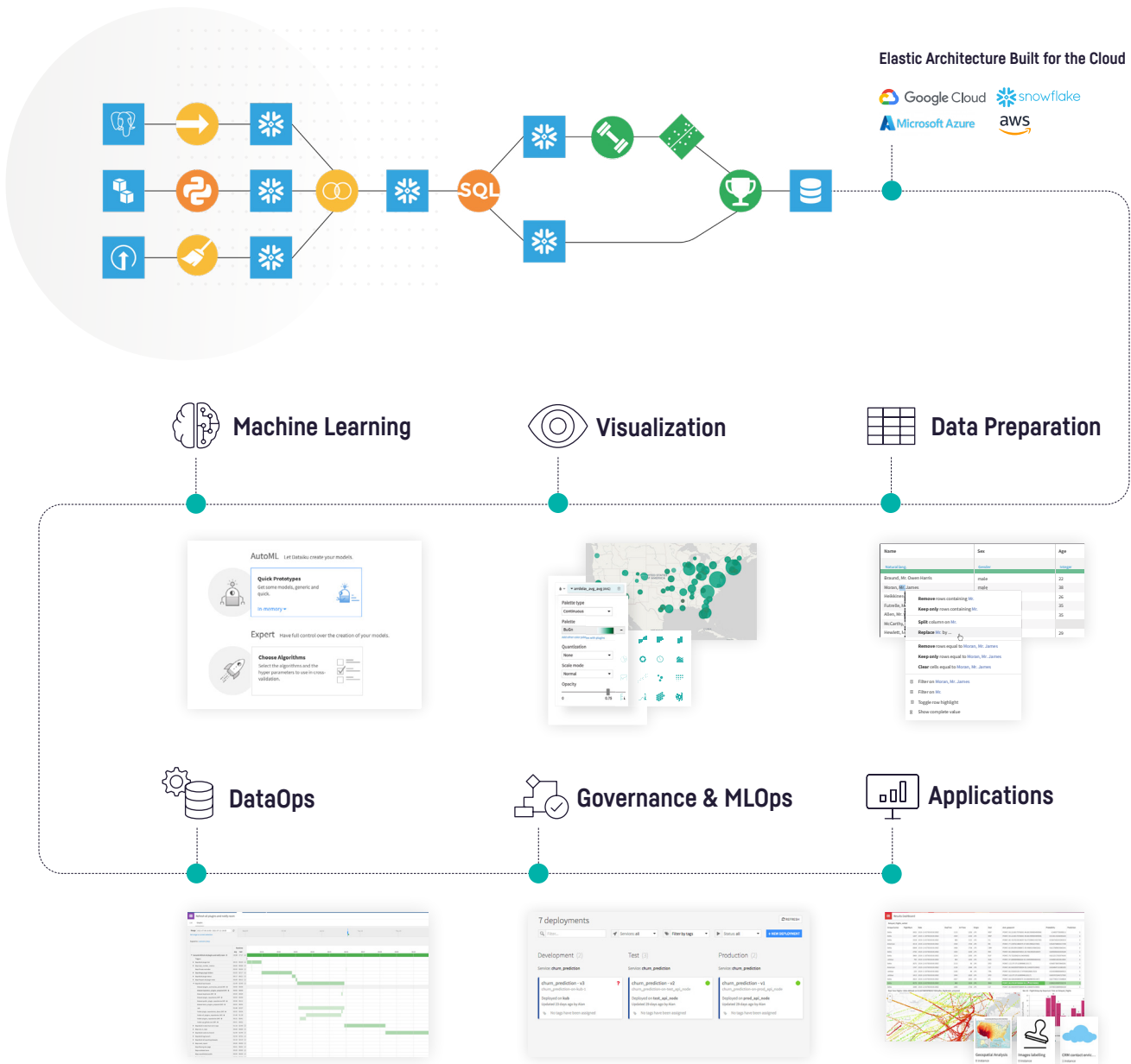


Mélanie Reversat

Based in Montpellier, France and the Director of Product Operations at Dataiku, Mélanie has been at the heart of the design and go to market of software in industries as different as semiconductor, video conferencing, agriculture, and now artificial intelligence.

As product manager, Mélanie has always kept in mind that facilitating the daily user experience and making it as understandable as possible is most important. An independent sponsor of the “Elles Bougent” association, Mélanie strongly believes in the importance of diversity in our tech environment.

Everyday AI, Extraordinary People



450+
CUSTOMERS

45,000+
ACTIVE USERS

Dataiku is the world's leading platform for Everyday AI, systemizing the use of data for exceptional business results. Organizations that use Dataiku elevate their people (whether technical and working in code or on the business side and low- or no-code) to extraordinary, arming them with the ability to make better day-to-day decisions with data.

