October 31 - November 2, 2023 | Orlando, FL

Hosted by OUC

UtilityAnalytics®

WEEK

Comprehensive Overview of MLOps and Governance

Alexander Johnson – Lead Data Scientist/ML Engineer

Logic20/20

Unlock the Universal Power of Data

#UtilityAnalytics #UAWeek

Utilities encounter substantial challenges when embracing ML solutions to enhance their operations and services

Utility Objectives With ML:

✓ Embrace Efficiency and Modern Ways of Working

✓ Manage Enterprise Risk and Promote Culture of Safety

✓ Maximize IT Investment Return

Challenges:

! Siloed projects

! Difficult path-to-value

! Managing Risk (IT and Enterprise)

Agenda

LOGIC 20/20

01 Overview Of ML Systems

02 Synergies of MLOps and Governance

03 Getting Started - Meaningful Accelerators

04 Tools for Governance

Overview of ML Systems (In the Wild)

LOGIC 20/20 experience a difference

What is Machine Learning?

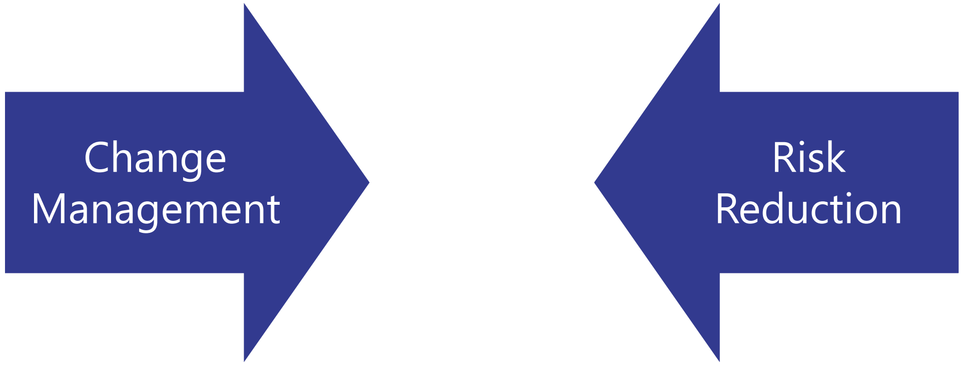
*A collection of statistical techniques that give computers the ability to "**learn**" a specific task from data without being explicitly programmed.*

Code + Data = Model

What is DevOps?

*"A set of practices intended to reduce the time between committing a change to a system **and the change being placed into normal production**, while ensuring high quality"*

-DevOps: A Software Architect's Perspective

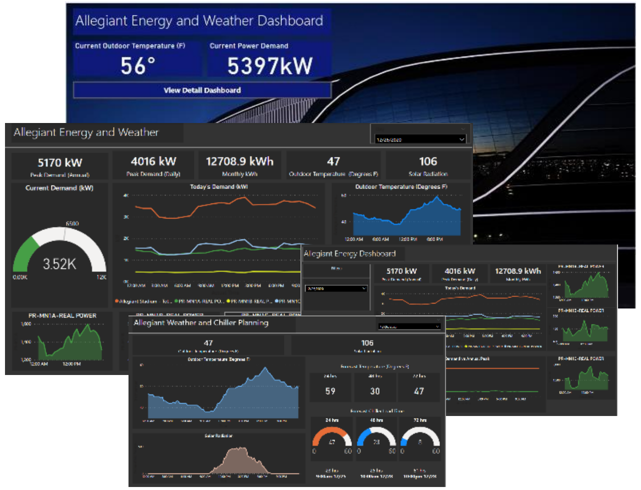


Change Management

Risk Reduction

What Can ML Offer?

BUSINESS INTELLIGENCE



Allegiant Energy and Weather Dashboard

Current Outdoor Temperature (F) 56°

Current Power Demand 5397kW

View Detail Dashboard

Allegiant Energy and Weather

5170 kW Peak Demand (Annual)

4016 kW Peak Demand (Daily)

12708.9 kWh Monthly kWh

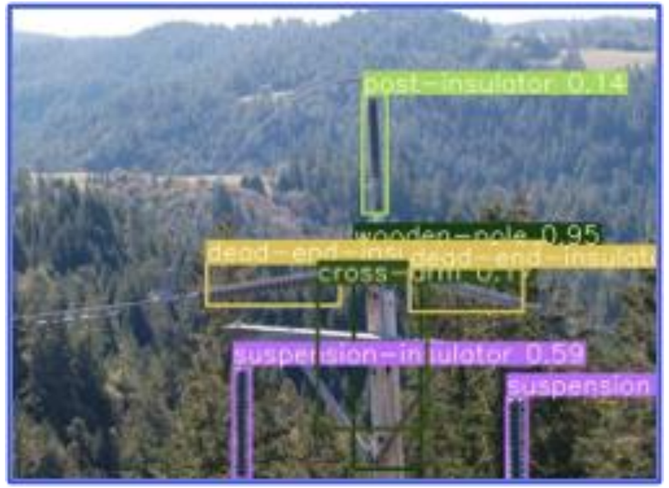
47 Outdoor Temperature (Degrees F)

106 Solar Radiation

Current Demand (kW)
3.52K
0.00K
12K
6500
Today's Demand (kW)
Outdoor Temperature (Degrees F)
PR-MN1A-REAL POWER
Allegiant Energy Dashboard
Allegiant Weather and Chiller Planning
Solar Radiation
59
30
47

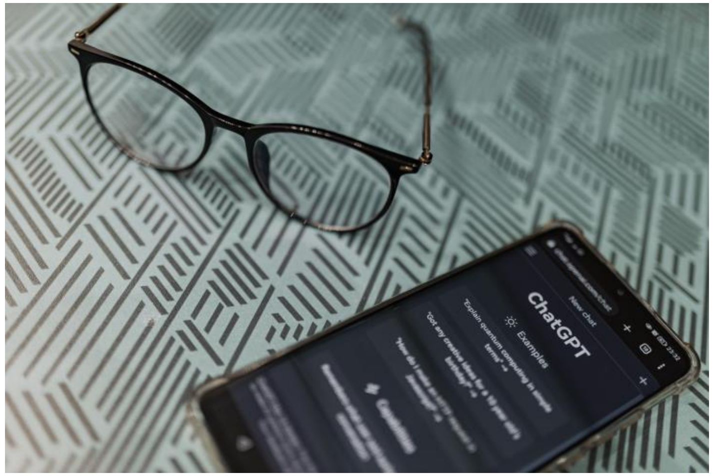
- Risk Analytics
- Load/Demand Forecasting
- Digital Twins
- Revenue Optimization
- Customer Insights

IMAGE ANALYTICS



- Asset Inspection
- Damage Assessment
- Vegetation Management
- Site Planning

LARGE LANGUAGE MODELS

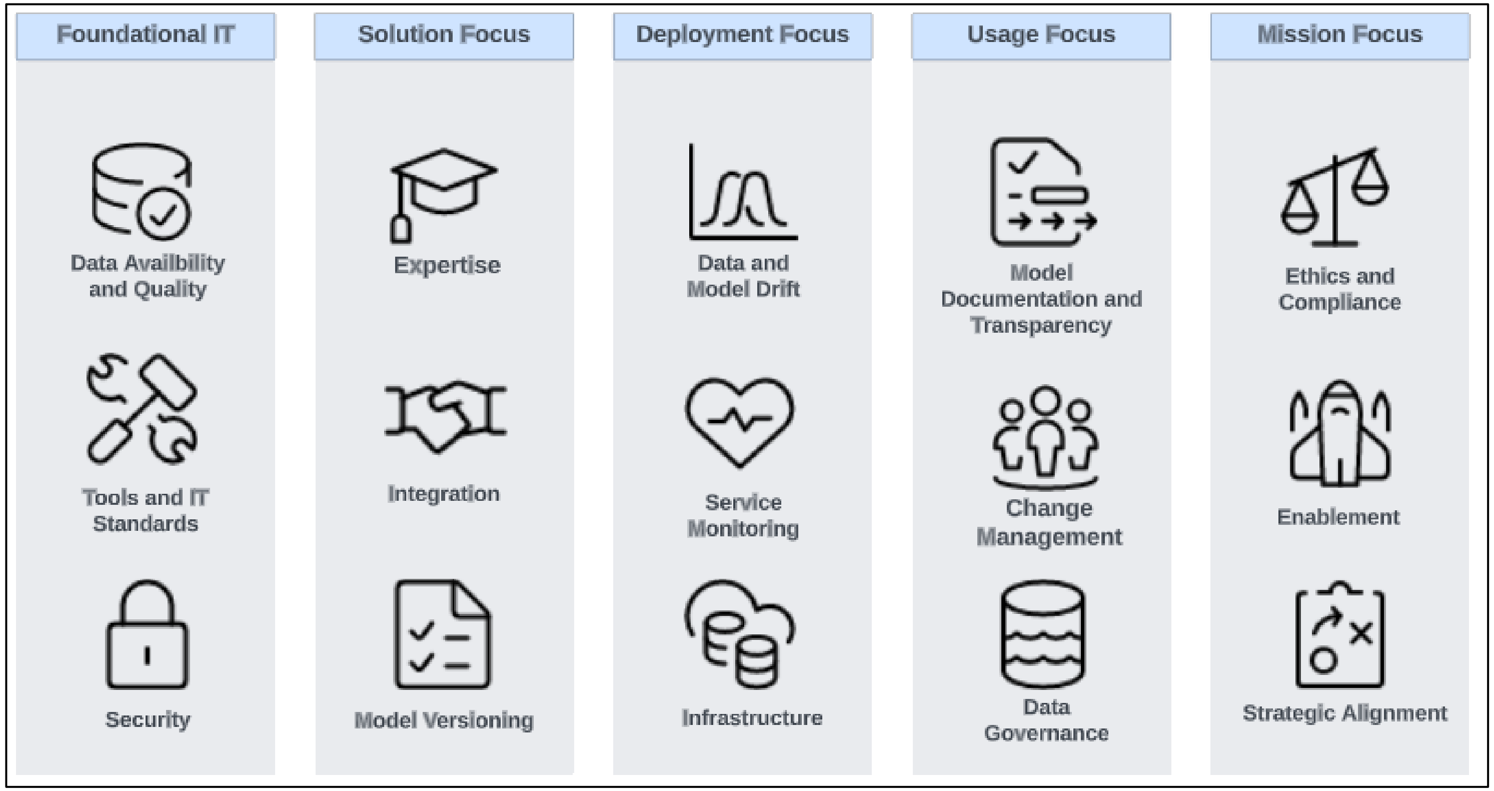


- Semantic Search/Document Retrieval
- Decision Support
- Customer Support

What Makes This Difficult? A Practical Example

Present Model

Future Challenges



Foundational IT	Solution Focus	Deployment Focus	Usage Focus	Mission Focus
Data Availbility and Quality	Expertise	Data and Model Drift	Model Documentation and Transparency	Ethics and Compliance
Tools and IT Standards	Integration	Service Monitoring	Change Management	Enablement
Security	Model Versioning	Infrastructure	Data Governance	Strategic Alignment

Steering AI Success – Compass and Engine

GUIDING AI STRATEGY AND ETHICS THROUGH GOVERNANCE

STRATEGIC DIRECTION

Define AI objectives and set a clear roadmap

ETHICAL AND COMPLIANCE OVERSIGHT

Establish guidelines for regulatory compliance and ethics in relation to AI adoption

IT ALIGNMENT

Align AI solution design standards with broader IT strategy

RISK MANAGEMENT

Identify and manage ML product lifecycle risks through organizational policies

FUELING AI EFFICENCY, POWERING INNOVATION THROUGH MLOPS

OPERATIONAL EFFICIENCY

Automated ML lifecycle and testing for streamlined operations

RELIABILITY

Operational ML metrics, including service latency, data quality and data drift are monitored

SCALE USE CASES

Templatized deployment patterns encourage reuse and align with IT standards

TRANSPARENCY

Models are versioned in centralized model registry – explainability metrics and model drift are tracked

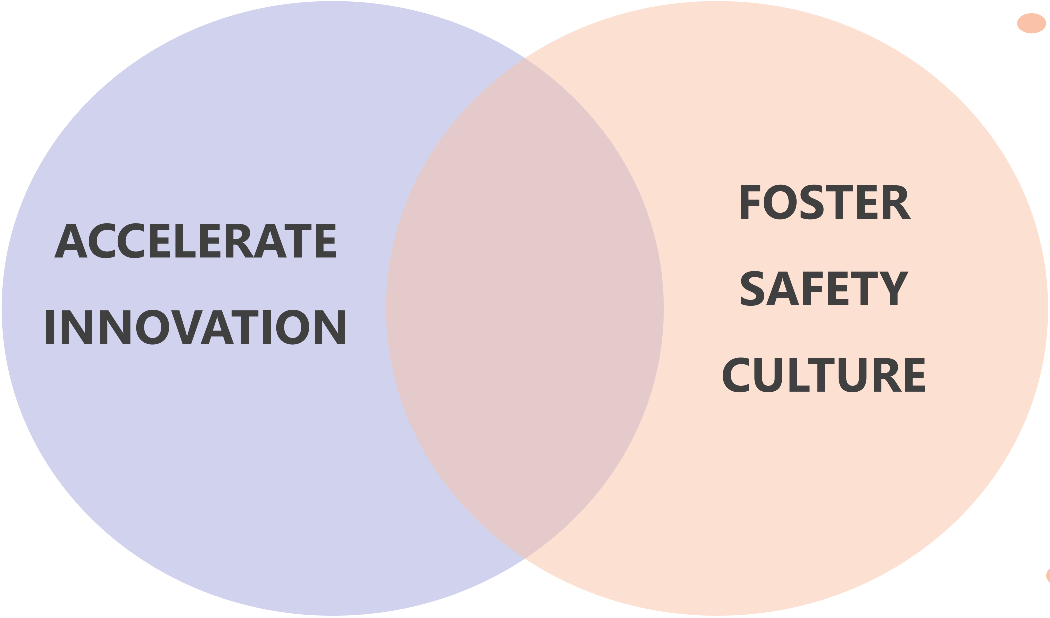
Approaches to Governance

Setting a Solid Foundation with MLOps

LOGIC 20/20

MLOps Activities		Governance Activities
Scale Design Patterns and Templates • Publish to central repository • Work with governance body for enterprise adoption	SCALABLE	**Enterprise-Wide Adoption** • Enable self-service provisioning of templates • Communication channels for best practices and insight
Automated Testing For Resiliency • System monitoring and alerting, monitor drift • Integration, reliability testing	RELIABLE	**Model Risk Management** • Risk assessments and management to mitigate internal and external concerns
Workflow Automation for ML Pipelines • Automation and versioning for all processes • Establish CI/CD practices	REPEATABLE	**Policy Enforcement and Auditing** • Automate compliance checks through ML Lifecycle • Periodic audits and assessments of process
Experimentation Platform • Build experimentation environment and scalable compute resources	PLATFORM	**Governance Platform Integration** • Reporting mechanisms for results • Standardize workflows
Data Connections • Establish secure connections to enterprise data sources to maintain integrity	DATA FOUNDATIONS	**Data Governance and Quality Assurance** • Focus on quality, lineage, security, and compliance • Defined ownership and access controls

Maximize the Impact of AI Adoption Responsibly Risk-Aware Accelerators



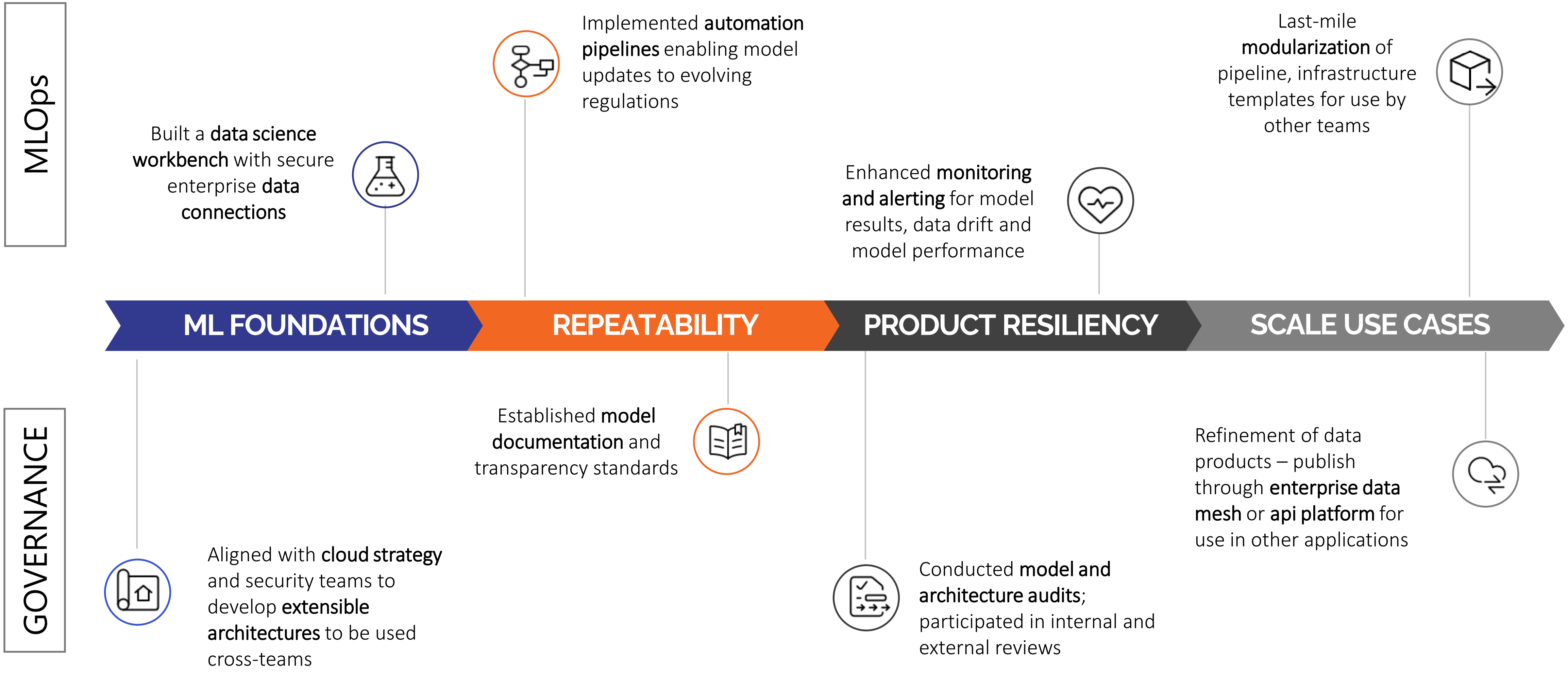
ACCELERATE INNOVATION

FOSTER SAFETY CULTURE

- Data Accessibility
- Workflow Automation
- Data Quality and Governance
- Solution Design Patterns and Templates
- Model Documentation & Transparency Standards
- Cross-Functional Teams
- AI Governance Boards
- Ethical AI Guidelines
- Regulatory Compliance Monitoring
- Security

experience a difference

Case Study: Maturing Wildfire Analytics



MLOps

Built a **data science workbench** with secure enterprise **data connections**

Implemented **automation pipelines** enabling model updates to evolving regulations

Enhanced **monitoring and alerting** for model results, data drift and model performance

Last-mile **modularization** of pipeline, infrastructure templates for use by other teams

ML FOUNDATIONS → **REPEATABILITY** → **PRODUCT RESILIENCY** → **SCALE USE CASES**

GOVERNANCE

Aligned with **cloud strategy** and security teams to develop **extensible architectures** to be used cross-teams

Established **model documentation** and transparency standards

Conducted **model and architecture audits**; participated in internal and external reviews

Refinement of data products – publish through **enterprise data mesh** or **api platform** for use in other applications

ML Governance – Beyond One Size Fits All

DEFINE OPERATING MODEL

Explicit definition of roles in cross-functional organizations delineate responsibilities and operating model for collaboration

ENGAGE AND SUPPORT

Owners of dependent workstreams provide support model to stakeholder teams

MONITOR AND ITERATE

Leverage metrics-driven approach to identify process bottlenecks and refine process

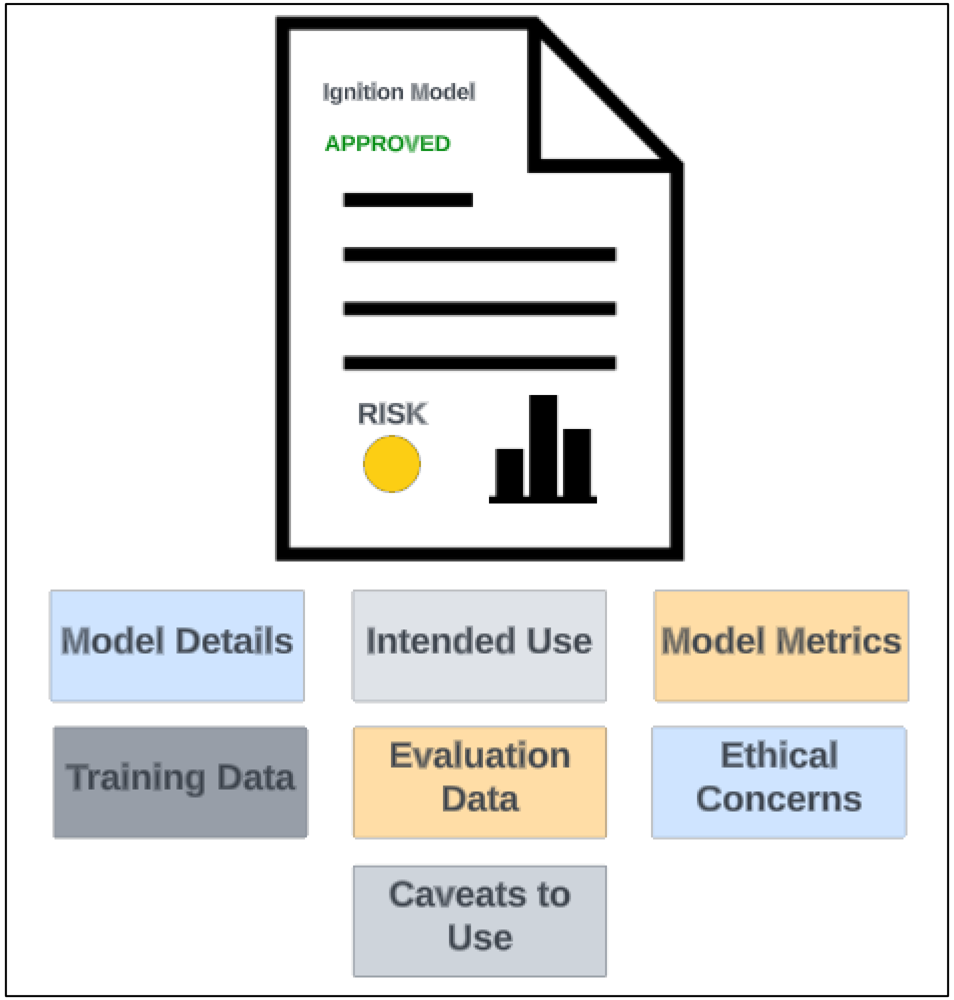
ML Governance Board

Develop Strategic Vision and Playbook

Ethical and Risk Oversight

Tool and Infrastructure Governance

Tools For Governance – Model Cards



Model Details

Intended Use

Model Metrics

Training Data

Evaluation Data

Ethical Concerns

Caveats to Use

RECOGNIZED BY KEY PLAYERS

- Originated from Google Research in 2019
- **Supported by Major Cloud Platforms** – GCP, AWS SageMaker, Azure (Preview)
- Embraced by Data Science Community (HuggingFace, Kaggle)

NO DEEP EXPERTISE NEEDED

- Consumable by all-regardless of domain and technical expertise
- Usage guidelines drive accelerators for **model reuse and transparency**

RISK AND COMPLIANCE

- Supports **proactive risk management** by disclosing limitations and potential challenges.
- **Eases regulatory reporting** by providing standardized information for audits and assessments

Tools For Governance – Risk Management Framework

LOGIC 20/20

CROSS-DISCIPINARY

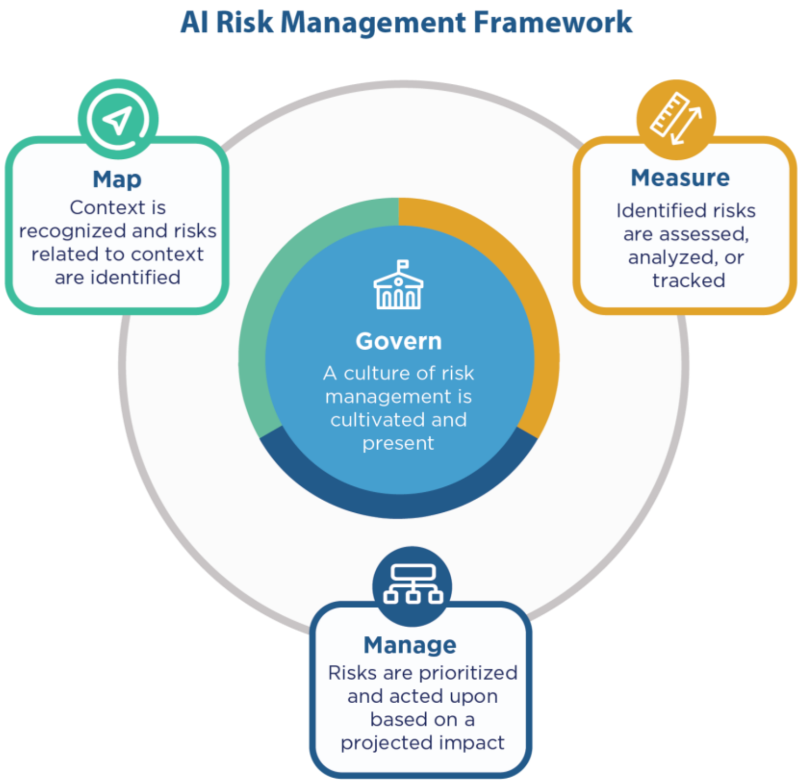
- First Release January 2023 under directive from US Congress
  - Developed by National institute of standards and technology
- Developed in collaboration with over 250 organizations private, public, academic, and non-profit sectors
- **Voluntary, Open, Non-Industry Specific**

GOVERNANCE AT CORE

- Transparency and Organizational Process to AI-driven activities
- Drive to approach to **map, measure, and manage risk** across all areas of the business

ORGANIZATIONAL LEVEL DIRECTIVES

- Build culture around **trustworthiness, responsible AI**, and enhance AI capabilities
- Include input and perspective for all AI Actors
- Structured Approach to Legal and Regulatory Compliance



AI Risk Management Framework

Map
Context is recognized and risks related to context are identified

Measure
Identified risks are assessed, analyzed, or tracked

Govern
A culture of risk management is cultivated and present

Manage
Risks are prioritized and acted upon based on a projected impact

NIST

Key Takeaways – How Do I Start?

Start Small With A Solid Foundation

- Prioritize use cases – inventory regulatory, ethical, and compliance risk factors
- Select meaningful, manageable pilots
- Develop plan how business will support models

Set North Star with Effective Governance

- Define strategy and establish roles
- Ensure alignment with organization values and industry standards

Maintain Momentum with Process and Tools

- Continuously refine processes and embrace automation
- Leverage modern tools and technologies
- Establish iteration cycle

THANK YOU

QUESTIONS?

Prior MLOps - (Hosted for UAI Members):
https://tinyurl.com/yww9j5xn