QuantUniversity, LLC

RESPONSE TO NIST'S ARTIFICIAL INTELLIGENCE RISK MANAGEMENT FRAMEWORK RFI

09/15/2021

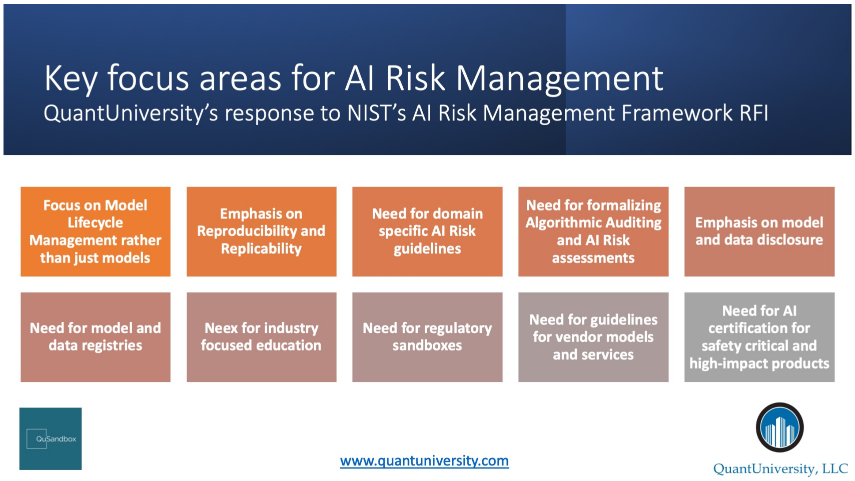
Contact: info@qusandbox.com

Executive summary

QuantUniversity is pleased to respond to NIST's AI Risk Management Framework RFI. As an AI-Risk focused company, QuantUniversity had had the opportunity to work with multiple organizations in setting up AI Risk Management frameworks and through its educational programs, has taught more than a thousand risk professionals on best practices in developing, auditing and evaluation of risk in AI and machine learning algorithms.

Based on our interactions with industry executives, academics and students, one of the key challenges we have identified is the operationalization and pragmatic application of AI frameworks. We call it the "implementation shortfall", considering the lack of formal guidance and established best practices in operationalizing AI Risk management.

Through the QuSandbox, QuantUniversity's platform for AI Risk assessment, evaluation and algorithmic auditing and with partnerships with organizations like PRMIA, QuantUniversity has helped students gain pragmatic knowledge on operationalizing AI principles into practice. Based on the learnings from the industry and our research in the area, the following are the key focus areas, we believe must be incorporated in the AI Risk management framework.



Key focus areas for AI Risk Management

QuantUniversity's response to NIST's AI Risk Management Framework RFI

Focus on Model Lifecycle Management rather than just models	Emphasis on Reproducibility and Replicability	Need for domain specific AI Risk guidelines	Need for formalizing Algorithmic Auditing and AI Risk assessments	Emphasis on model and data disclosure
Need for model and data registries	Neex for industry focused education	Need for regulatory sandboxes	Need for guidelines for vendor models and services	Need for AI certification for safety critical and high-impact products

QuSandbox

www.quantuniversity.com

QuantUniversity, LLC

Thank you again for the opportunity to present QuantUniversity's views and for your attention.

Sri Krishnamurthy

QuantUniversity

Summary

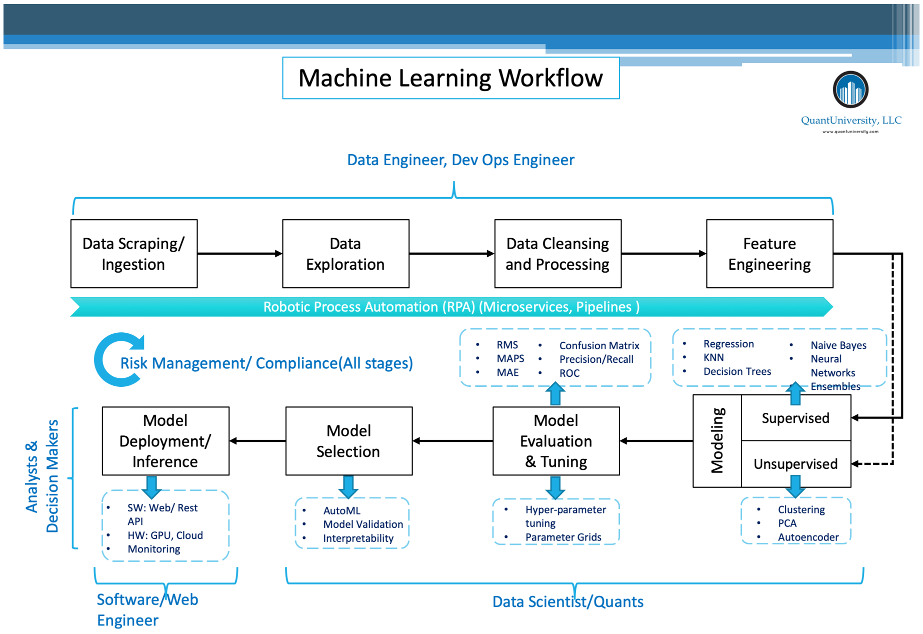
As machine learning and AI has permeated every facet of our lives, innovations that were inconceivable just a decade ago have been realized. The rapid pace of growth and adoption of technological advances has enabled fascinating applications but has also meant that the risks have grown. Without a formal, pragmatic AI risk management framework, we are bound to see failures and mishaps that may not have been intended during design and deployment. It is our responsibility to ensure that AI systems have undergone a comprehensive AI risk assessment to understand the various risks and practical actions taken to mitigate and control the various risks associated with such systems.

Fortunately, these issues have been prevalent in today’s discussion. Companies and academic researchers have been researching various themes of AI risk and solutions proposed to address potential risks. Various explainability, bias detection and mitigation tools, monitoring solutions and the whole area of MLOPs have garnered significant attention. The number of conferences and publications are testament to the growing interest in the area to understand and solve various issues in the area of AI risk.

While there has been many commendable projects, products and proposals, it is necessary to take a holistic approach and not address areas in a piece-meal manner. In addition, one of the common complaints in the industry is that while many AI risk evaluation and mitigation frameworks sound reasonable and agreeable, there is very little guidance on how to pragmatically implement them in the industry. Since the area is new, there aren’t many established best practices to bank upon. Education is another delta where; industry practitioners find it difficult to apply academic research into practice.

Based on our discussions with various students and industry practitioners, we propose the following ten key focus areas to be considered while formulating and AI Risk Management framework at NIST.

1. Focus on Model Lifecycle Management rather than just models



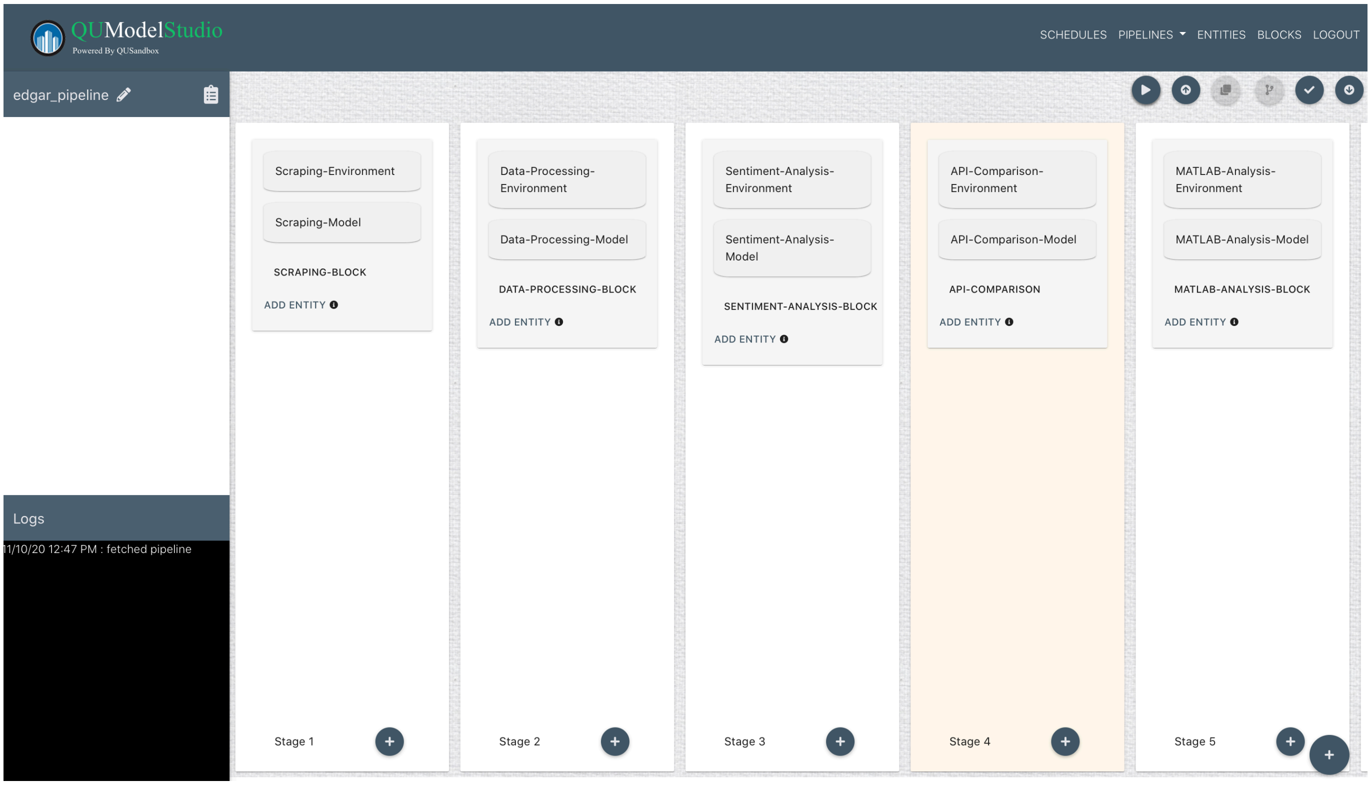
Copyright www.quantuniversity.com 2019

A lot of emphasis has been placed on machine learning models both in the industry and academia. Metrics and monitoring tools are focused on the performance of the model. However, when deploying AI and ML systems in the industry, the entire pipeline, starting from data to the predictions are important. Since most machine learning and AI applications are data-driven applications, every processing step contributes to the final outcome/predictions. This includes risk. Risk assessments and management must factor the entire pipeline rather than just the modeling piece.

The AI risk management framework must focus on the entire model life cycle rather than just the AI/ML models.

2. Emphasis on Reproducibility and Replicability

As most AI systems are built end-to-end using pipelines, it is important to ensure these pipelines are reproducible for risk evaluation and assessment. The reproducibility crisis in science[2] is a reality in AI and ML systems too! As a model validator, we have seen how difficult it is to reproduce tests.



```
11/10/20 12:47 PM : fetched pipeline
```

Technologies like Docker and pipelining tools have made it feasible to ensure reproducibility factors all four key areas: data, models, environment and process and not just model reproducibility.

The AI Risk Management Framework must emphasize reproducibility and replicability as a part of risk evaluation and analysis.

3. Need for domain specific AI Risk guidelines

Context and domain specificity is extremely important for AI risk management. While generic guidelines work well for certain applications, AI applications that are specific to use cases needs to be evaluated factoring the nuances of those areas.

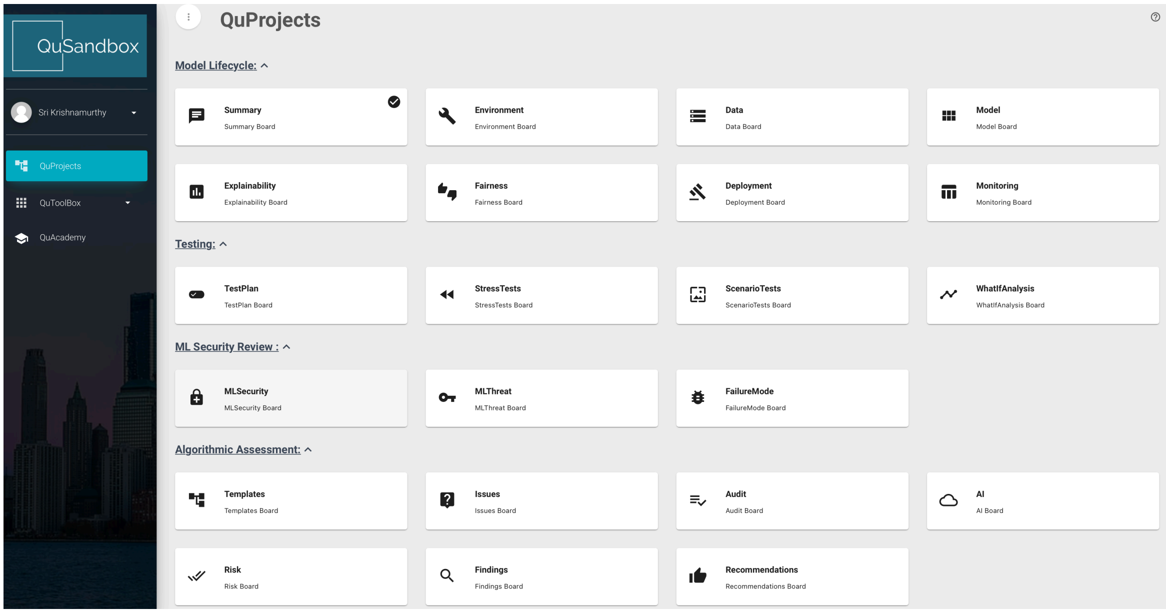
While healthcare and safety critical applications need more scrutiny, applications in marketing like personalization or recommendation may not require the same level of rigor. We have heard pushback from companies who are building AI systems that AI risk management isn’t something they would invest in currently without guidelines or regulation for their industry.

The AI Risk management framework should enable domain-specific guidelines to ensure that adoption is feasible and is contextual to the business practice.

4. Need for formalizing Algorithmic Auditing and AI Risk assessments

While organizations build capabilities both technical and non-technical, it is important to recognize that all organizations may not have the same bandwidth to build teams to conduct AI risk assessments inhouse. Third-party Algorithmic auditors, who specialize in areas may be able to provide a more comprehensive assessment of risks and may be able to provide best practices to organizations that are small and new to AI risk management. However, without regulation and industry adopted standards and best practices, it is difficult to draw a line on what AI risk assessments should encompass.

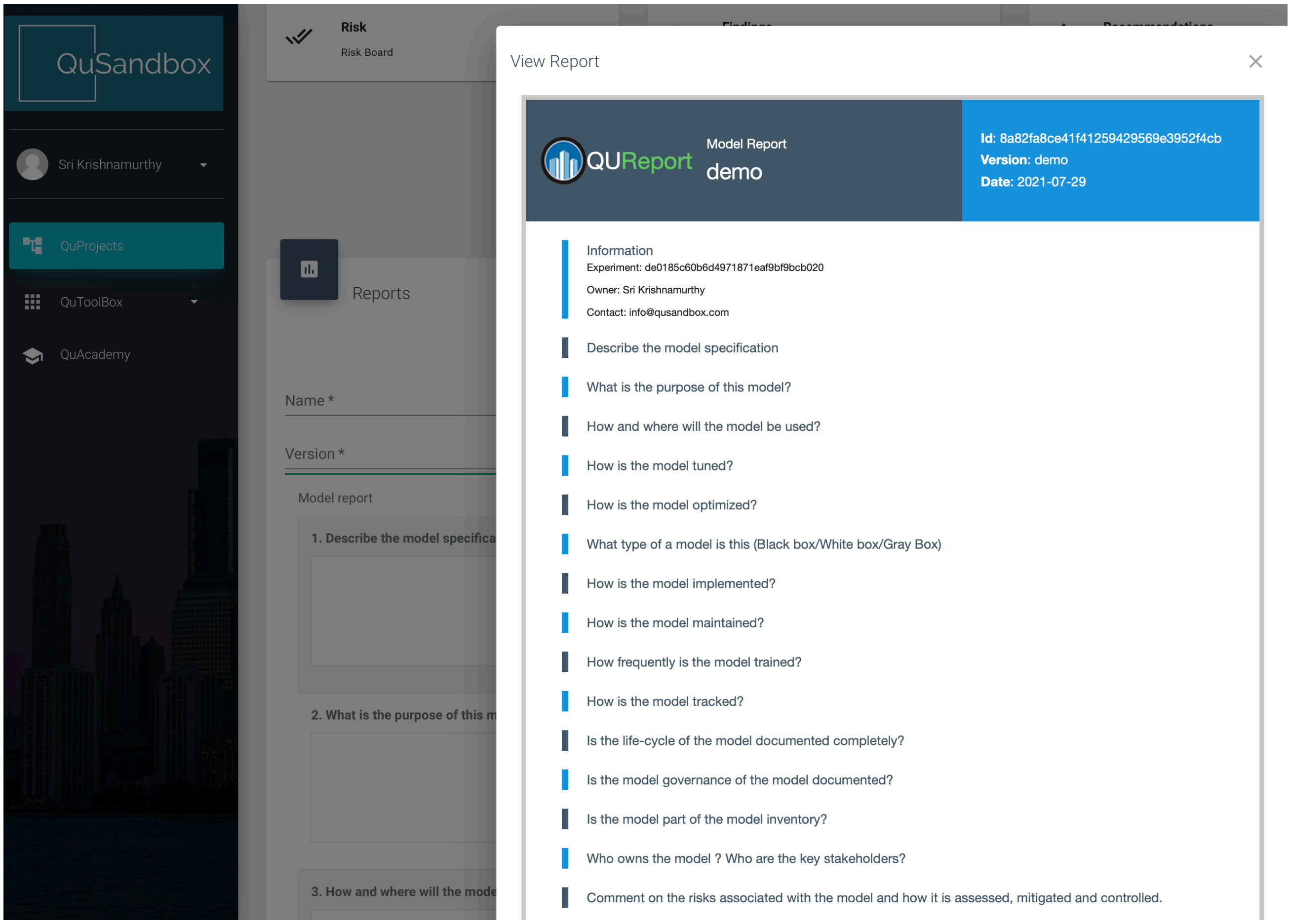
We at QuantUniversity have built QuSandbox for risk assessments and we contextualize these to the needs of our clients.



Comprehensive guidelines on algorithmic auditing and AI risk assessments would help both independent auditors and companies to pragmatically incorporate AI risk assessments into their practice.

5. Emphasis on model and data disclosure

We have observed that most companies building AI and ML systems use proprietary and open-source tools and build pipelines for their specific use cases. Many models we evaluate have skeletal documentation on the models and data used to build these models. Without standards and expectations of disclosure and being accountable, AI accidents are bound to happen. In our educational programs at QuantUniversity[3], we strongly emphasize the need for formal documentation and disclosure. This is especially important for blackbox and vendor models.



Model Report
demo

Id: 8a82fa8ce41f41259429569e3952f4cb
Version: demo
Date: 2021-07-29

Information
Experiment: de0185c60b6d4971871eaf9bf9bcb020
Owner: Sri Krishnamurthy
Contact: info@qusandbox.com

Describe the model specification

What is the purpose of this model?

How and where will the model be used?

How is the model tuned?

How is the model optimized?

What type of a model is this (Black box/White box/Gray Box)

How is the model implemented?

How is the model maintained?

How frequently is the model trained?

How is the model tracked?

Is the life-cycle of the model documented completely?

Is the model governance of the model documented?

Is the model part of the model inventory?

Who owns the model ? Who are the key stakeholders?

Comment on the risks associated with the model and how it is assessed, mitigated and controlled.

We believe the AI Risk management framework must provide guidelines for model and data disclosures.

6. Need for model and data registries

AI systems have multiple tools, data sources, versions, configuration parameters, metadata that are impossible to manage without a concerted effort to manage all key components of the model life cycle. In addition, with model development and deployment becoming more and more agile, the risk of model failures have been increasing. For models that are made available as a service, both internal and external, we believe, a formal registry of models is required to ensure the model deployment processes are rigorously evaluated and risks assessed formally. This will also help in any post-mortems or evaluations if unexpected events occur.

We have been working on building **QuTrack** to register deployed models and datasets.

We believe the AI Risk Management framework should provide guidelines on model and data registries including model inventories to ensure standards and protocols are established in this novel area.

7. Need for industry focused education

With AI and machine learning still in its early stages of infancy, there is a huge dearth of in-house knowledge within companies to actively manage AI projects. The job-boards of the day illustrates the need for AI and ML talent within companies. Schools and universities are focused on programs in AI and machine learning. Bootcamps and online programs are emerging to fill in the gap.

However, most offerings of the day are focused on fundamentals and don't provide a comprehensive and contextual industry focused education track that are relevant and can be pragmatically applied. We at QuantUniversity focus primarily in the financial industry and have worked with organizations like the CFA institute and PRMIA to create educational programs that are contextual and focused in areas such as algorithmic auditing, stress testing, model risk management etc. [3]

We believe there is an opportunity to foster industry-focused, domain specific education that would benefit industry practitioners augment and expand their skills in the area of AI and machine learning particularly in the areas of AI risk management which is new in various industries

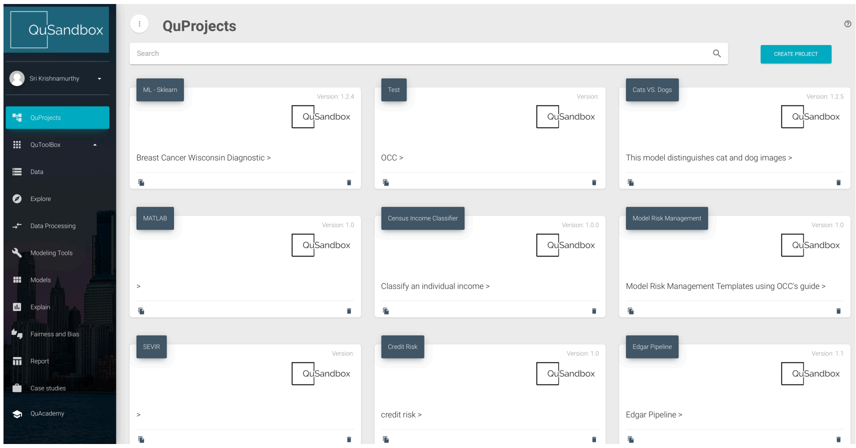
The AI risk management framework should detail topics and concepts or initiate additional efforts to foster industry educational programs within specific domains.

8. Need for regulatory sandboxes

With AI and machine learning growing significantly in the industry, without regulation and industry best practices, many untested products are becoming part of critical infrastructure within companies. With untested open-source products, without comprehensive testing guidelines, companies are acquiring AI products without sufficient vetting.

While larger companies can build teams to do due diligence, smaller companies are “trusting” product vendors to have done due diligence. In addition, with lack of transparency, there are many unknown risks companies take without realizing the impact. For use cases, where there is a systemic impact and large groups of population could potentially be using these untested products, there are significant repercussions.

While regulatory efforts are growing in Europe, US and other areas, it is important to emphasize the need for regulatory sandboxes to test and vet out AI products prior to deployment. We are building **QUSandbox** for exactly this purpose.



QuProjects

ML - Sklearn
Version: 1.2.4
QuSandbox
Breast Cancer Wisconsin Diagnostic >

Test
Version:
QuSandbox
OCC >

Cats VS. Dogs
Version: 1.2.5
QuSandbox
This model distinguishes cat and dog images >

MATLAB
Version: 1.0
QuSandbox
>

Census Income Classifier
Version: 1.0.0
QuSandbox
Classify an individual income >

Model Risk Management
Version: 1.0
QuSandbox
Model Risk Management Templates using OCC's guide >

SEVIR
Version:
QuSandbox
>

Credit Risk
Version: 1.0
QuSandbox
credit risk >

Edgar Pipeline
Version: 1.1
QuSandbox
Edgar Pipeline >

We believe, there is an opportunity to build guidelines for AI Risk management that could be tested out in Sandboxes prior to deployments as a part of the AI Risk Management Framework

9. Need for guidelines for vendor models and services

The AI ecosystem is growing and there are thousands of vendors providing AI and machine learning products either as tools or as services. Without formal guidelines and regulation, it is left to the companies incorporating these products or the end-consumer to do the due-diligence of whether the products work to specification or as advertised.

With complexity increasing and the proliferation of Blackbox models, and without disclosure and formal expectations from vendors, it is becoming a challenge to enterprises to set standards on what vendors should disclose and publish when providing AI models and services.

The AI Risk Management Framework should provide guidelines for vendor models and services and expectations of risk assessments they have conducted prior to deployment of their services.

10. Need for AI certification for safety critical and high-impact products

As applications like Autonomous driving, health applications and financial decision-making systems all using AI, we are reaching a point where there could be unanticipated AI accidents that could have significant negative effects on large user groups and populations. We strongly believe safety critical and high-impact products that use AI must be certified by agencies. With lack of regulation and novelty in the area, we believe NIST's AI risk management framework would be a great opportunity to broach the subject and foster discussion and engagement on the important topic of AI certification.

We strongly urge NIST to incorporate guidance on AI certification in the AI Risk management framework.

Conclusion

While we have discussed the ten focus areas we believe are important, reviewing comments by other industries and academic organizations, we strongly believe that this effort by NIST is commendable and we than NIST for the opportunity to contribute our thoughts to this effort.

Additional themes are discussed in our brief "*The New Decalogue: Model Risk Management Revisited" [1] and other QuantUniversity publications and whitepapers.*

REFERENCES:

1. https://www.quantuniversity.com/publications.htm
2. https://www.nature.com/articles/533452a
3. https://www.quantuniversity.com/courses-landing-page.html

ABOUT QUANTUNIVERSITY

QuantUniversity is a quantitative analytics advisory focusing on the intersection of Data science, Machine learning and Quantitative Finance. We take a practitioner’s approach to working with pragmatic applications of frontier topics to real-world financial and energy problems. QuantUniversity advises various companies in Quant Finance application development, validation and in algorithmic auditing. QuantUniversity is pioneering the next generation platform called QuSandbox for Algorithmic auditing that supports anonymization, model escrow and tracking, synthetic data generation, reproduction and experimentation

QuantUniversity is a proud member of the LF AI & Data Foundation and a member of NVIDIA's Inception Accelerator program.

To get started right away, just tap any placeholder text (such as this) and start typing.

HEADING 2

View and edit this document in Word on your computer, tablet, or phone. You can edit text; easily insert content such as pictures, shapes, and tables; and seamlessly save the document to the cloud from Word on your Windows, Mac, Android, or iOS device.

> *“Quote”*

Use styles to easily format your Word documents in no time:

- For example, this text uses the List Bullet style.
- On the Home tab of the ribbon, check out Styles to apply the formatting you want with just a tap.