# Feedback for NIST AI Risk Management Framework – The Critical Need for a Paradigm Shift

Prodago is pleased to submit the following feedback to the request for information by the National Institute of Standards and Technology ("NIST") on the AI Risk Management Framework ("AI RMF"). Prodago commends NIST for undertaking a consensus-driven, collaborative approach to enhance the NIST AI RMF. The guidance provided by this framework will help technologists, users, regulators, and stakeholders of AI systems at large build AI that is effective, compliant, secured, and principled.

NIST AI RMF has a place in norms setting on building robust and trustworthy processes in AI design, development, and deployment, and bridging the gap between current methodologies and new techniques of an AI-tailored risk management framework. As evident from the multitude of AI failures (80% of AI systems do not go into production[1], and high-profile cases of AI failures[2]), current methodologies of building AI systems could risk unintended consequences.

## Introduction: The Challenges of AI Risk Management

Prodago is a data and analytics governance startup (Gartner 2x cool vendor for information governance) with the mission to enable all advanced analytics teams with operationalizing responsible AI through effective, compliant, principled, and secure operating practices. Through a combination of AI governance, risk management, compliance, capability building and policy setting tools and solutions, Prodago allows teams to operationalize and scale trust to prioritize, plan, execute and monitor trustworthy AI development and deployment. Prodago also comes equipped with a body of knowledge of 2,500+ operating practices (Prodago Governance Accelerators) combining global data and AI regulations, standards, and best practices, giving teams an operational playbook and a path towards successful ROI on AI.

Developing AI systems inherently require different perspectives as designing, developing, and deploying these automated systems are fundamentally different from previous expert systems, and require clear positioning of principles that translate to robust operational practices to realize responsible AI. One of the main challenges of AI risk management is the diversity of risk perspectives and risk impacts. This diversity leads to incomplete risk frameworks, unclear impacts (and business case to act) and undefined responsibilities to mitigate the risks. Hence, success in managing AI risks is a team sport and requires successful business transformation to adequately address the challenges.

To focus on clarity of our comments, we are structuring this document addressing the core questions as requested by NIST's current draft with our recommendations. For any questions, please contact Mario Cantin, CEO and Chief Data Strategist of Prodago.

[1] *Driving ROI Through AI - ESI ThoughtLab*. (n.d.). Econsult Solutions, Inc. Retrieved Apr 20, 2022, from https://econsultsolutions.com/roi-ai/

[2] *Artificial Intelligence Incident Database*. (n.d.). Incidentdatabase.ai. Retrieved Apr 20, 2022, from https://incidentdatabase.ai/apps/discover

## QUESTIONS FROM NIST AI RMF DRAFT

### 1. Whether the AI RMF appropriately covers and addresses AI risks, including with the right level of specificity for various use cases.

----------------------------------------------------------------

In the NIST AI RMF, it would benefit to additionally cover 3 AI risk topics:

- *Lack of business perspective*. AI risk structures are often centered on *Inadequate usage of AI*, *Consequences of AI usage*, *Privacy-Security-Ethic considerations* and on *Model Performance*. AI RMF lack all the perspective related to business adoption, resistance to change, trust, transformation, project selection and alignment with business objectives. It is a mistake. These risks represent the major causes for AI failure to deliver expected value.
- *AI risks vs. Data Risks*. There is a strong dichotomy between AI Risks and Data risks. Data is strictly considered as an input to AI processes and something that can be managed independently. This dichotomy can be explained by the over focus of data risks on quality aspects. Data & AI risks should be managed as a whole.
- *Lack of management risks*. When it comes to the management of AI, several disciplines are involved: Architecture, Data Science, Privacy, Data Quality Management, Security, Ethics, etc. Organizations have different levels of maturity in each of these disciplines and often very low maturity in some disciplines. AI RMF fail to include risks related to deficiencies and low maturity in organization management capabilities. AI 'management' risks can be used very efficiently as a driver to prioritize and improve management capabilities.

**Recommendations**:

1. Enrich AI RMF with the following risk topics: business adoption, resistance to change, trust, transformation, project selection and alignment with business objectives
2. Enrich AI RMF with risks specific to data attributes (quality, metadata, lineage)
3. Enrich AI RMF with risks related to deficiencies in data management (data quality management, data privacy management, metadata management, ethical management, etc.) and risks related to deficiencies in enterprise positioning (lack of policies and directives – ethics, privacy, retention, etc.)

Why is it so important to include these risks? Because it addresses the ultimate risk – the risk of failure, and not achieving ROI of the project.

There is an opportunity (and a need) to use AI risks as a driver to organizational transformation and capability building. To achieve this, AI RMF must explicitly include the risks that impact AI ROI. That includes specifically the risks related to deficiencies in data management. AI risks typically focus on avoiding / reducing the potential impacts of risk materialization.

Beside inadequate usage of AI and its consequences, AI risks management must also include the risks related to organizations not achieving their targeted ROI (Return on

Investment) on AI. This risk perspective leads to the definition of risks related to low maturity, lack of guidance (policies, principles, etc.), lack of collaboration, undefined accountabilities, resistance to change, lack of trust.

80% of AI initiatives never go to production. The average ROI on AI initiative is only 1.3%. Organizations recognize this fact and want urgently to mitigate this risk. The mitigation of these risks implies numerous actions to be taken and several new capabilities to be built by organizations. It means that beside aiming to avoid impacts of AI risk events, AI risk framework can also explicitly include risks related to deficient management capabilities.

In order to use AI risks as a driver for transformation, the risk granularity, structure, and taxonomy must allow a direct connexion between the risk and the targeted actions. Due to the challenges of fragmentation, low maturity, and AI adoption, it is imperative that AI risks explicitly address deficient / low maturity in all facets of AI management.

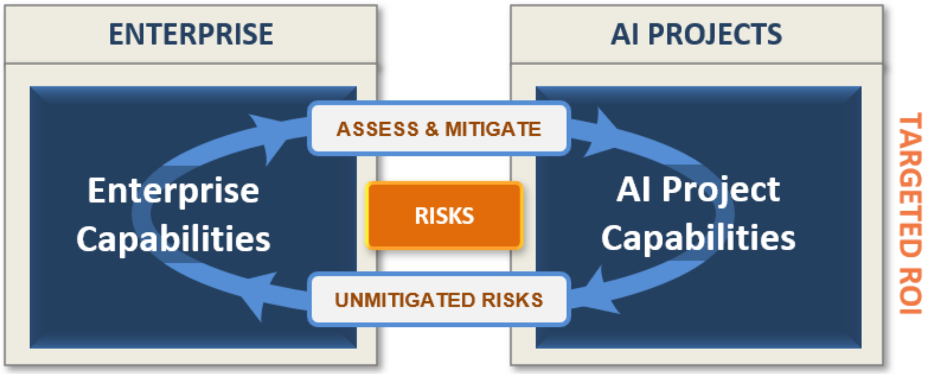

Diagram 1. LEAN DATA & ANALYTICS GOVERNANCE

This lean approach allows to link targeted ROI to risk mitigation, aligning AI risks with business value at risk. AI risks and their weight on targeted ROI become a business case element and a prioritization factor for organizational transformation and capability building.

prodago

Prodago has developed the Lean Data & Governance framework with the specific objectives of enabling business transformation. The idea of using value at risk in projects as a driver to improve organizational capabilities is a direct reaction to the failure of governance efforts, disconnected from organizational priorities and struggling to demonstrate value. The Prodago framework includes a comprehensive AI risk register that includes the risks related to transformation, resistance to change and ROI at risk.

Prodago was selected as a *Gartner Cool Vendor – Information Innovation and Governance* in 2016.

**3. Whether the AI RMF enables decisions about how an organization can increase understanding of, communication about, and efforts to manage AI risks.**

**7. What might be missing from the AI RMF.**

**8. Whether the soon to be published draft companion document citing AI risk management practices is useful as a complementary resource and what practices or standards should be added**

-----------------------------------------------------------------

**Enriching the Govern Function of NIST AI RMF**

**Recommendations**:

AI RMF must improve its capacity to enable decision making, specifically on the aspects of risk mitigation capability building, risk mitigation planning and execution by AI projects.

Prodago considers the following challenges to this capacity:

a) The management of several types of AI risks involves a high level of maturity of organizations. Security, Privacy, Ethics and Data Literacy are often supported by vastly different level of organizational capabilities. This means that risk assessment and risk mitigation are not adequately supported by organizational positioning, principles, policies, directives, and guidelines.
*Example. An AI project is asked to define how it will manage the risks related to data retention. Organizations are often not providing clear guidelines (e.g., Data Retention schedule) or do not have the capability to understand the specificities of AI projects*.

b) Lack of skills by the 1st line to mitigate the risks. AI risks are highly fragmented, and several specialized topics must be addressed. Organizations are usually embarking on an AI journey where the adoption and maturity will grow over several years. It means AI project are ill-equipped to address all the risks. It also means that a 2nd line throwing too many risks at the first line will be welcomed with a lot of resistance and that such an exercise would strongly put the business case of all AI initiatives at risk.

These challenges are particularly seen in organizations where a 2nd line of defence (risk management) will require the 1st line (AI team) to assess and mitigate risks. Improving the structure of AI risks is a first step. Improving the capability assess and mitigate risks is as critical.

**Recommendations**:

The AI RMF should be enriched with mitigation activities, and related accountabilities, for each risk. Pre-defined mitigation activities truly support organizations in making the decisions about improving their capability to mitigate risks. The idea is to recognize the inability and the need of organizations to build their capability to address and mitigate risks

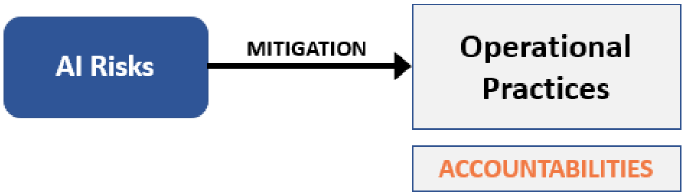

Diagram 2. MITIGATION ACTIVITES FOR AI RISKS

## Enriching the Map Function in NIST AI RMF

AI RMF enriched with mitigation activities can be used to bring decision making on AI risks at a very operational level. See below how an AI RMF with mitigation activities (operational practices) can be used, in an organization, to operationalize AI risk management in project context.

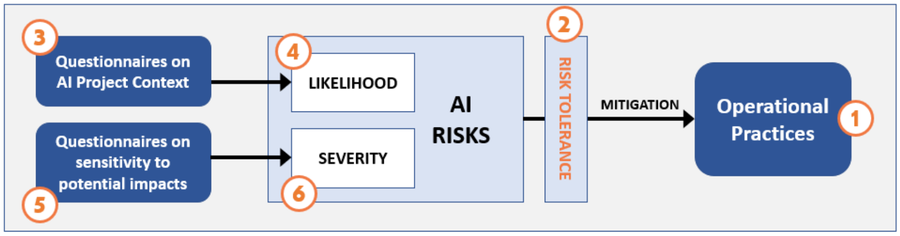
3
Questionnaires on AI Project Context
Questionnaires on sensitivity to potential impacts
5
4
LIKELIHOOD
SEVERITY
6
AI RISKS
2
RISK TOLERANCE
MITIGATION
Operational Practices
1

Diagram 3. USING QUESTIONNAIRES TO PRESCRIBE MITIGATION ACTIVITES

1. For all risks that include potential impacts at the organization level (e.g., Privacy breach), define the risk tolerance.
2. Define questionnaires, to be filled by AI projects, that describe the nature and the context of the project (use case, targeted technology, type of data used, type of data sources, sharing of data, types of users, level of expertise, etc.)
3. Use question answers as an input to the likelihood of occurrence of risk events. For example, if the project is not using any Personal Information, certain privacy related risks will have a probability of occurrence that is null or incredibly low.

4. Define questionnaires, to be filled by AI Projects, that assess the sensibility of the project to different topics (e.g., Sensibility to poor operational data quality might be low if the project is only a proof-of-concept).
5. Use question answers as an input to the severity of the risk events. For example, very low sensibility to operational quality will lead to very severity of Risks related to operational data drifts.
6. Using answers to the questionnaires, prescribe mitigation activities to the project for the risks above the risk tolerance thresholds.

Using an AI risk management framework that includes predefined mitigation activities for each AI risks enable organizations to compensate for low maturity in many AI risk related disciplines. It also allows them to quickly understand and assess the mitigation capabilities that are not supported or do not exist in the organization. Unmitigated risks are a strong driver to organizational changes because they link in a very direct way expected benefits to business value at risk.

An AI risk management framework that includes mitigation activities opens the possibility to decomplexify the assessment and mitigation processes. It allows organization to evolve in their risk mitigation capabilities at a pace connected to their appetite for AI successes and achieved ROI.

prodago

Prodago has developed a comprehensive register of more than 2,000 operational practice, managed in a SaaS solution. More than 150 AI risk events are mapped to the key operational practices that mitigate the risks. Prodago has also developed questionnaires for AI projects where the answers directly modulate the likelihood and severity of risks. Mitigation activities are prescribed to the project based on configured risk tolerance.

**5. Whether the AI RMF is in alignment with or leverages other frameworks and standards such as those developed or being developed by IEEE or ISO/IEC SC42.**

-----------------------------------------------------------------

The AI RMF is in alignment with the other frameworks and standards developed or being developed. However, AI RMF lack proper interoperability mechanisms with the frameworks, standards, laws, and regulations to allow continuous alignment and facilitate implementation. The consequences of deficiencies of interoperability between AI RMF and AI frameworks, standards, laws & regulations are severe.

**Recommendations**:

An interoperability mechanism can be created through processes and accountabilities. It means each statement of a law or standard should be translated into the specific operational practices (and related accountabilities) required to operationalize it. A similar exercise should be done to identify the specific operational practices (and related accountabilities) required to mitigate risks.

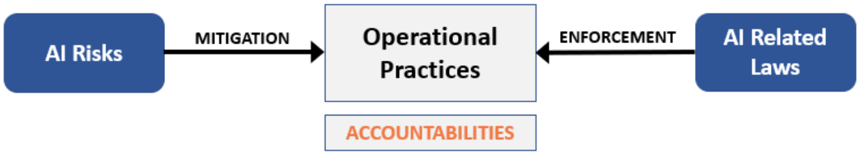

Diagram 4. OPERATIONAL PRACTICES AS INTEROPERABILITY MECHANISM

This simple approach has several key benefits:

- It provides an operational language to interpret AI related laws
- By decoupling the operational practices from the law, the same operational practices can be mapped to several laws. It creates the organizational agility to manage alignment with the multiple new laws and regulations being published.
- The operational practices can be assessed to understand the organization operational readiness toward certain laws.
- The operational practices required to mitigate risks might also be required to align with certain laws. If the operational practices do not exist, it strengthens the business case to create them.
- The operational practices can be aligned with the level of maturity of the organization, providing an incremental approach to operationalization.

This approach can be extended to increase other interoperability perspectives.

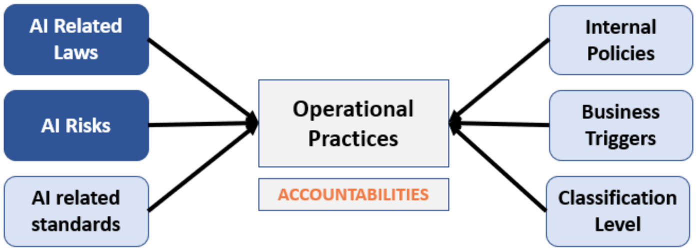

Diagram 5. OPERATIONAL PRACTICES AS AN ENHANCED INTEROPERABILITY MECHANISM

When transposed to the AI risk management framework context, this approach leads to a connexion between mitigation actions and compliance requirements

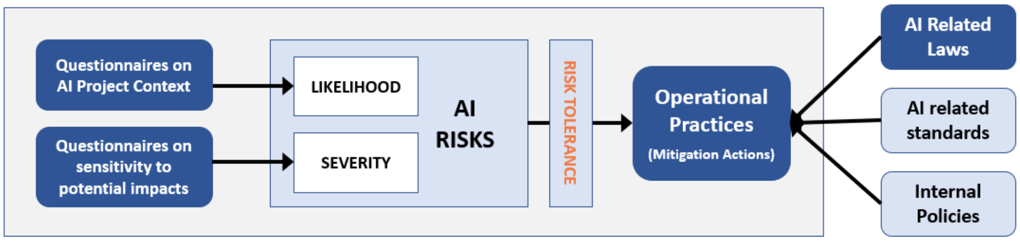
Questionnaires on AI Project Context
Questionnaires on sensitivity to potential impacts
LIKELIHOOD
SEVERITY
AI RISKS
RISK TOLERANCE
Operational Practices (Mitigation Actions)
AI Related Laws
AI related standards
Internal Policies

Diagram 6. CONNECTING MITIGATION ACTIONS TO COMPLIANCE REQUIREMENTS

Prodago has developed a comprehensive register of more than 2000 operational practice, managed in a SaaS solution. More than 50 global laws, regulations and standards are mapped to the operational practices, as well as the complete Prodago AI risk register.