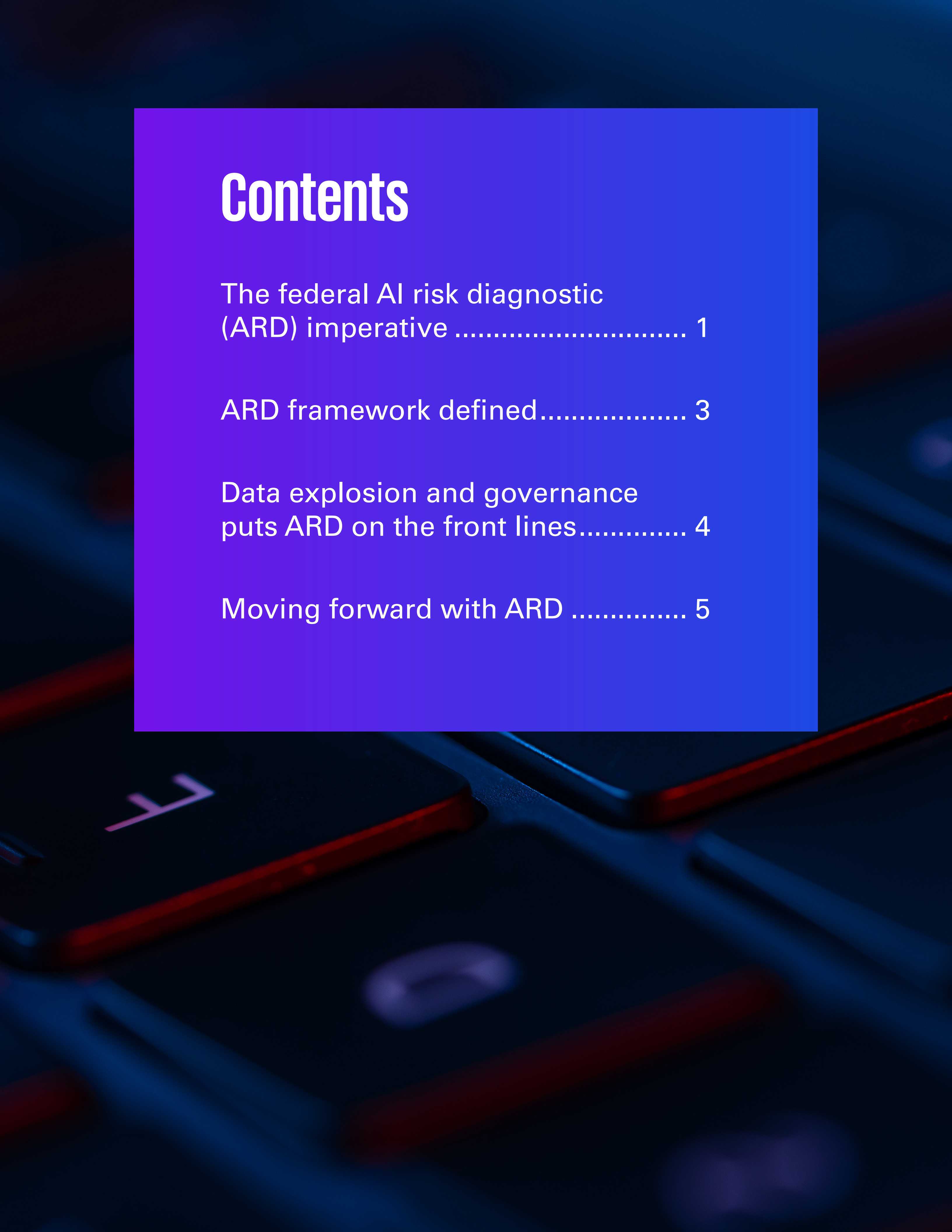
KPMG

Enabling trust in the AI revolution

Driving mission value in the new reality with a federal AI risk diagnostic framework

KPMG Accelerated AI Risk Diagnostic Services –
We build trust.

kpmg.com/us



Contents

The federal AI risk diagnostic (ARD) imperative

Technology is continuing to move at a rapid pace across the federal government. Artificial Intelligence (AI), Machine Learning (ML), and blockchain technologies are unlocking predictive insights, enabling automation, and driving unprecedented efficiencies while reducing the potential of fraud, waste, and abuse. These technologies offer the capability to make government operations more agile, improve mission outcomes, and enhance transparency in areas ranging from emergency preparedness to providing better health and human services. At the same time, governments at all levels must carefully consider policies that help maximize the advantages of AI and reduce inherent risks. Some AI-related challenges include the development of effective approaches to address characteristics of AI and ML trustworthiness, including equity, accuracy, reliability, transparency, fairness, and mitigation of any biases, as well as unintended harmful uses.

The exponentially increasing rate of technology change over the last several years is not a one-time phenomenon or trend; rather, it represents a paradigm shift in how government must adapt, evolve, and improve. We have also learned that unprecedented global events, such as the COVID-19 pandemic, continue to influence government decisions, drive agencies to reimagine service models, and elevate the importance of a sustainable, scalable, and future-ready technology environment.

As with any transformation, the rapid deployment of new AI processes and technologies without appropriate risk perspective and standards raises important questions that government agencies need to consider:

- What if our AI-based models entail data bias?
- What if our AI-based models entail cognitive bias?
- What if our AI-based models entail algorithmic bias?
- What if we don’t have clear accountability around who needs to identify bias in AI systems and programs?
- What if we do not have reliable sources of training data?
- What if we do not have an adequate framework for identifying and mitigating societal risk attributable to potential AI bias?

Trends requiring attention

- Explosion of data
- Growing digital complexity
- Rapid pace of AI adoption and increasing applications of ML
- Stringent AI accountability guidelines and standards by GAO (GAO-21-519SP) and NIST (NIST.SP.1270)
- Emphasis on social and health equity
- Reliance on connected devices
- Accelerated cloud adoption

In this new reality, dynamic and well-managed technology deployment is a clear modernization requirement, enabling agencies to control key technology risks without stifling innovation. Without a doubt, employing an ARD framework should be considered an organizational imperative.

A comprehensive ARD framework should be considered an important component of an overarching AI governance methodology as it addresses the risks driven by emerging technologies. Organizations that deploy an ARD as a component of their decision-support system, rather than just for the sake of regulatory compliance mandates, are positioned to achieve better operational results, empowered by prudent use of technology.

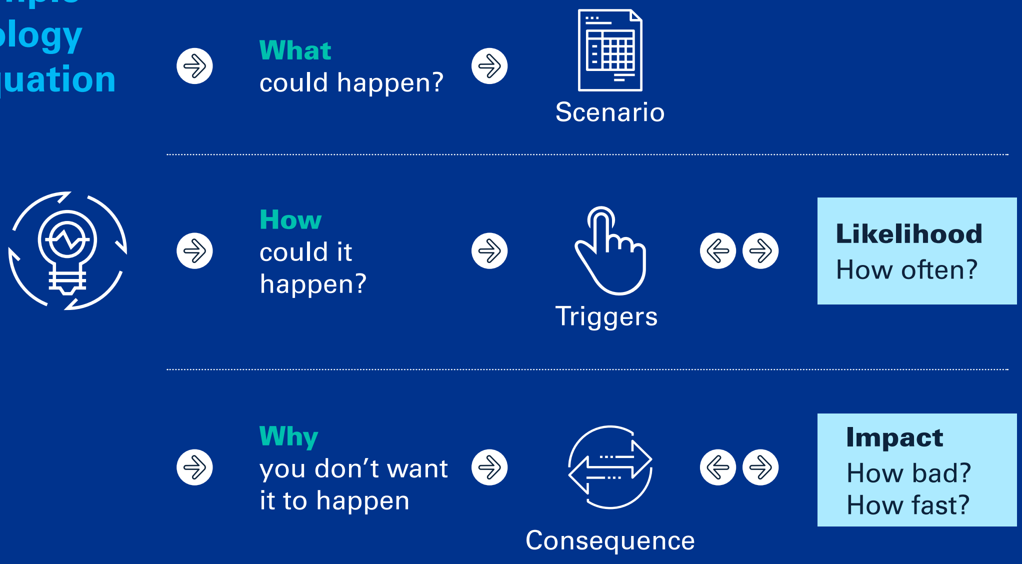
A strategic, effective, and flexible ARD framework helps organizations:

- Facilitate trustworthy and equitable AI
- Build stakeholder confidence in technology spend
- Earn citizen trust while capitalizing on new solutions and emerging technologies

According to the 2020 KPMG Global Emerging Technology Survey Report,

59% of technology and business executives say that the pandemic has created an impetus to accelerate their digital transformation initiatives.

The simple technology risk equation



What could happen? → Scenario

How could it happen? → Triggers ↔ **Likelihood** How often?

Why you don't want it to happen → Consequence ↔ **Impact** How bad? How fast?

ARD framework defined

An ARD framework is part of an AI governance methodology focused on identifying, assessing, managing, monitoring, and reporting on operational, financial, and regulatory risks related to the ownership, deployment, and use of AI.

The ARD framework considers the top AI and ML-related risks in an organization, and the various triggers and consequences of those risks, to help government agencies understand:

- Risks, vulnerabilities, and threats to individuals, organization, and society
- Responsible, equitable and governable AI principles
- AI accountability and traceability considerations
- Quality of data sets used to develop, train, and drive the AI and ML algorithms
- Integrity and fairness of the algorithmic-based decisions
- Fostering public trust in AI by addressing potential biases.

The ARD framework is enabled by technology, data, and people and serves as a component of the overarching technology risk management (TRM) framework. The program enables managers to address accountability and responsible use of AI and ML in government programs and processes, as specified in the guidelines issued by Government Accountability Office (GAO) and NIST.

The program addresses key considerations for federal agencies and other entities that are considering, selecting, and implementing AI and ML systems.

KPMG's view is that that technology empowers government, and AI is enhancing, accelerating, and automating key decision-making for federal agencies, enabling government employees to spend their time on higher-value activities: however, legacy risk management programs are unable to keep up with the pace of advancement in AI. An ARD framework can enable organizations in adopting technology in an accelerated yet responsible manner.

Next-generation ARD framework is emerging.

While most organizations already possess the talent and tools to manage traditional technology risk, and are even actively doing so, what's missing is the strategic alignment of AI into a well-managed framework.

Top AI and ML risks to manage

- Statistical or data bias
- Social and health equity
- Systemic bias
- People and skills
- Third-party technology and services
- Transparency and trust
- Services and reliability
- Emerging technologies
- Governance and performance
- Regulations and compliance with GAO and NIST

Data explosion and governance puts ARD on the front lines

COVID-19 pandemic fueled a new era of exponential technology innovation, empowered by AI, to automate operations and unlock efficiencies in all aspects of business, including the government sector. However, this creates new and unique challenges of oversight and governance for federal managers.

During the initial COVID-19 response phase, agencies rapidly accelerated the deployment of remote working, AI and ML models, and data analytical tools but often without adequate governance and controls. Risks include:

- If the underlying data is incomplete, biased, or inconsistent, it can negatively impact the accuracy and integrity of the algorithm result.
- AI and ML algorithms require massive quantities of data, and not all agencies have access to such data. Also, privacy regulations may limit the use of classified or sensitive data.

As agencies move forward with the new reality, AI teams are leveraging initial lessons learned to optimize and secure algorithms and ML models. There is a critical need for rolling out new governance models, and controls to ensure that the new way of working is fair and equitable. This includes:

- Developing a centralized process for the deployment of AI and ML models
- Enhancing security operations, especially limiting training model access to sensitive data
- Developing AI and ML working protocols, threat identification, and escalation processes
- Applying controls in response to how employees use AI technology to make decisions
- Addressing systemic, human, and statistical biases via training and education
- Digitizing AI risk and controls activities.

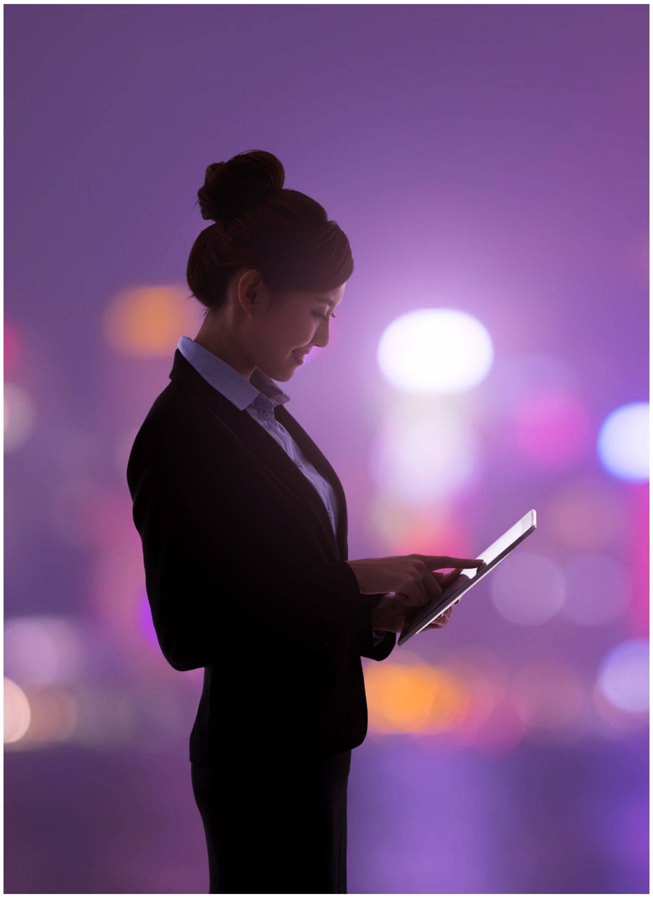
What's on the mind of government executives?

According to the 2021 Thriving in an AI World Survey Report,

92% of government executives agree it's important for government agencies to have an AI ethics policy, though only 53% say their own organization has one

67% of government executives say it's hard to stay ahead of the constantly evolving AI landscape

63% of government executives say they think the U.S. is lagging other countries in terms of AI adoption



Moving forward with ARD

As AI adoption accelerates across the federal government, there is growing recognition of both its strengths and limitations. Incorrect design or usage of AI can expose an agency to operational, financial, regulatory, and reputational risks. New regulations and guidelines are emerging that will guide agencies on how to address trustworthiness of AI technologies, and systems, products, and services. Maintaining the status quo isn't an option. Government agencies need to be more proactive in assessing and managing their AI risk posture. An ARD framework will establish more trust in AI to gain confidence in mission-critical decisions, ensure your AI systems satisfy your operational requirements, and derive sustained value from your AI.

Interested in learning more about how an ARD framework can reduce your agency's AI vulnerabilities and compliance requirements? KPMG's specialists can help.

Viral Chawda
Principal
vchawda@kpmg.com

Mike Peckham
Managing Director
mpeckham@kpmg.com

kpmg.com/socialmedia