FORVIS®

AI Regulatory, Compliance and Contracting Issues

2023 Insurance Virtual Seminar

Meet the Presenters

Chuck Hollis

Partner – Technology Transactions

Norton Rose Fulbright US LLP

chuck.hollis@nortonrosefulbright.com

Sean Christy

Partner – Technology Transactions

Norton Rose Fulbright US LLP

sean.christy@nortonrosefulbright.com

FORVIS

Agenda

- Setting the Stage
- State of Regulation in the US
- Areas of Liability and Risks
- Enterprise Governance
- Third Party AI Systems

Key terms

FORVIS

What makes AI problematic?

Its complexity means AI system likely to be provided to companies that deploy it (users) by an expert third party service provider (provider)

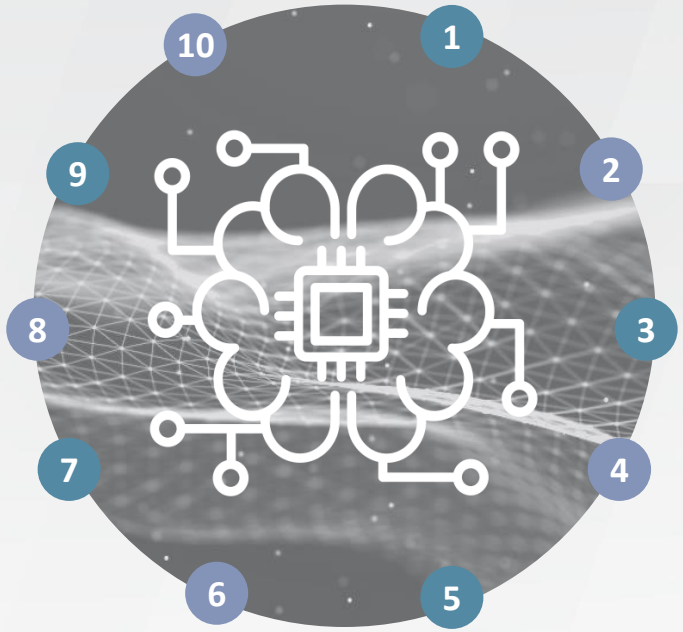
Socio-technical systems:
AI technology + people + processes

Some AI can continue to learn (and change the model parameters) from the input data it is processing in the field, becoming autonomous unless monitored or constrained

Where the Model is fixed, the world can change and the outputs become inaccurate, so monitoring necessary

The mathematical relationships the AI uses to predict/create output range from easy to describe and follow, and/or reflective of our accepted real world causality, to so complex most humans cannot understand them and/or seemingly at odds with our accepted real world causality

Using complex and uninterpretable AI may not be suitable in a number of situations (e.g., where opportunities will be denied and decision subjects cannot alter their behavior to obtain such opportunities because the determinative factors are not known)



Digitization and automation of service delivery (with or without AI) is making ex ante human oversight and intervention unattractive as slow and expensive

Wide rapid roll out: impact many

Historic data (including relationships) – model (including relationships) – input data – output data (new content/prediction based on relationship)

Human may never have detected relationships before - may/may not be stronger/more reliable than the reasons humans have seen or believed caused the desired outcome

The model does not explain why the relationship occurs in the historic data: this needs to be interpreted and described by a human

If historic data was non-representative or biased the model will reflect this (without intervention)

Without human intervention the model will have no safety, legal or morality constraints:

- if AI system output used without further human checking/interpretation and without the ability to retake a flawed decision – all safety, legal and morality constraints will need to be coded in
- if good human oversight and understanding of how the AI works and how accurate it is, fewer constraints could be coded in as the human could introduce them (i.e. override/disregard AI prediction) when required (if alert and diligent)

FORVIS

State of regulation in the US

- Federal Action and Legislation
- State of Local Laws and Regulations
- State Data Privacy Laws
- Local Action
- State Level and Sector Level Guidance

2023 Insurance Virtual Seminar

Federal action and legislation

FORVIS

Federal action and legislation

- There have been several attempts at legislation at the Federal Level:
  - Algorithmic Accountability Act of 2023 (reintroduced on September 21, 2023)
    - Originally introduced in 2019 and then again in 2022
  - American Data Protection and Privacy Act – (ADPPA) (2022)
  - Data Privacy Act of 2023 (Financial Services)
  - AI Insights Forum (Led by Senator Schumer)
  - Bipartisan Framework for U.S. AI Act (Senators Blumenthal and Hawley)
  - Protect Elections from Deceptive AI Act (Senators Klobuchar, Hawley, Coons and Collins)
  - Federal Artificial Intelligence Risk Management Act of 2023 (November 2023 – Senators Warner and Moran)
  - Numerous others……almost weekly / daily

FORVIS

Executive Branch Guidance

- Blueprint for an AI Bill of Rights: Making Automated Systems Work for the American People (October 2022)
- Executive Branch Action (DOL, EEOC, DOJ, FTC, CFPB, DHHS, OCC, FDIC, SEC)
    - NIST – AI Risk Management Framework
    - National AI Research Institutes

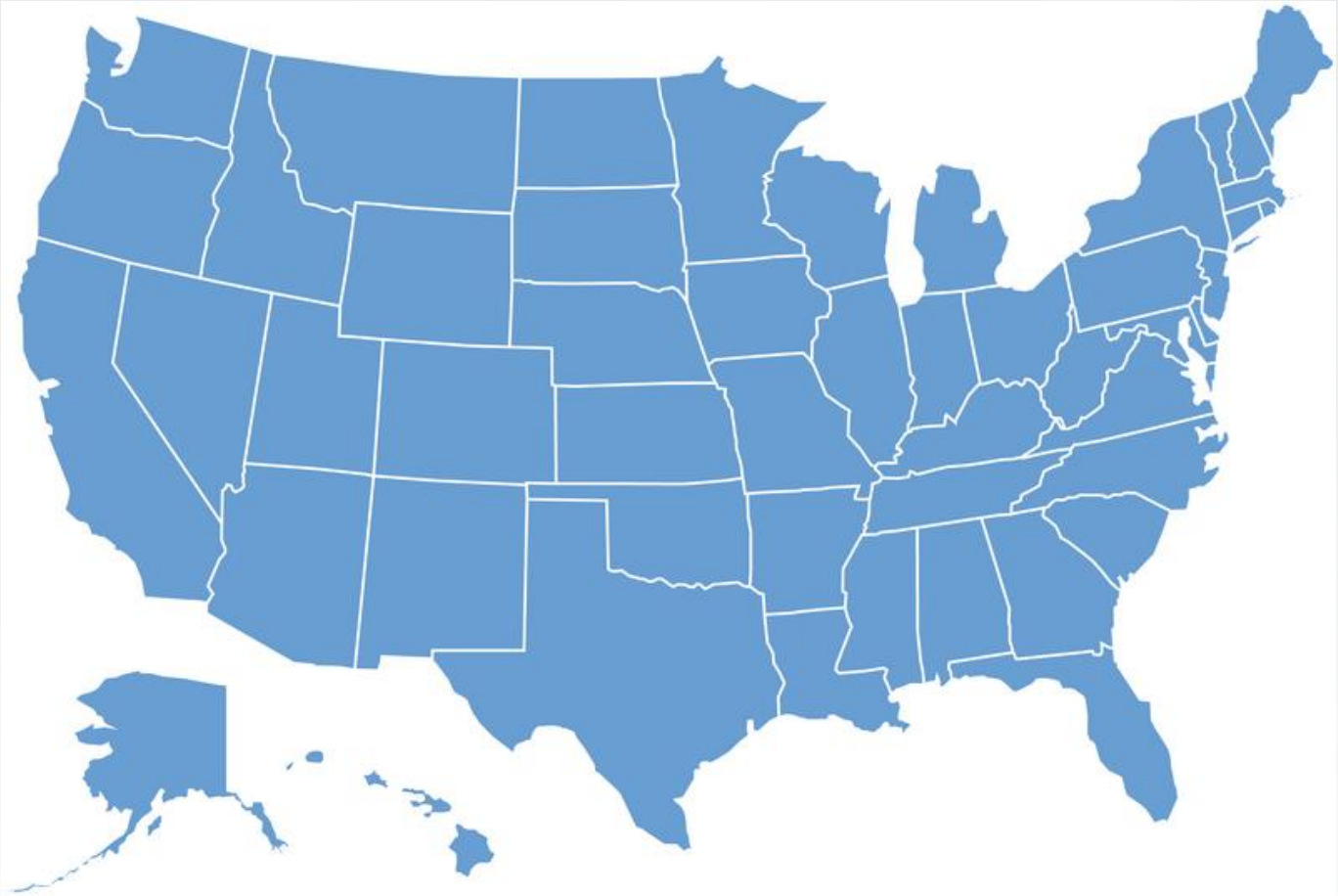
- Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence (White House – October 30, 2023)
    - New Standards for AI Safety and Security
    - Protecting America's Privacy
    - Advancing Equity and Civil Rights
    - Standing Up for Consumers, Patients, and Students
    - Supporting Workers
    - Promoting Innovation and Competition
    - Advancing American Leadership Abroad
    - Ensuring Responsible and Effective Government Use of AI

Note that the Federal Artificial Intelligence Risk Management Act of 2023 is an attempt to codify some of the Executive Order.

FORVIS

State of regulation in the US

Where does that leave us?



We are left with a patchwork of various state and local laws and actions

FORVIS

State and local laws and regulations

The State Legislatures have been active in 2023.

At least 25 states and territories have introduced bills or regulations related to AI (excluding facial recognition and autonomous vehicles).

Colorado Department of Insurance (CDI)

- CDI issued Final AI Regulation – Effective as of November 14, 2023
- Governs algorithms and models that use external consumer data and information sources (ECDIS)
- Applies to life insurers that use ECDIS or ECDIS based models
- Required to implement risk-based governance and risk management frameworks
- Directed at identifying and remediating unfair discrimination
- The Final AI Regulations prescribes certain components for the framework

State data privacy laws

Some State Data Privacy Laws provide for the right to "opt out" of "profiling" or other "automated decision-making," and require businesses to conduct data privacy impact assessments. Others have AI relevant provisions.

- California Consumer Privacy Act (CCPA) / California Privacy Rights Act (CPRA)
- Colorado Privacy Act
- Connecticut Data Privacy Act (also limited sourcing of AI by the State)
- Virginia Consumer Data Protection Act
- Others in 2023 (Indiana, Montana, Tennessee and Texas)
- Other states had pending / failed legislation that follow these acts

FORVIS

Be mindful of local laws and regulations

New York City (Local Law 144) – Prohibition on Automated Employment Decision Tools – Requires the technology to undergo a bias audit each year. (Effective in 2023).

State level and sector level guidance (sampling)

- NCSL (National Conference of State Legislatures) – Approaches to Regulating Artificial Intelligence – A Primer (August 2023)
- NAIC (National Association of Insurance Commissioners) – Principles of Artificial Intelligence (September 2020)
- NAIC – Exposure Draft of the Model Bulletin on the Use of Algorithms, Predictive Models, and Artificial Intelligence Systems by Insurers (Published July 2023 – Comments accepted until September 2023)

FORVIS

State of regulation in the US

European Union

- EU AI Act: Classification system to determine level of risk
  - unacceptable / banned (generally prohibited except in rare circumstances)
  - high risk (significant governance obligations and assessments)
  - generative AI (requires compliance with transparency requirements
  - limited risk and minimal risk (more limited requirements, e.g., monitoring / transparency)

Similar to GDPR – Global companies need to be aware of EU regulations.

FORVIS

FORVIS®

Areas of liability and risk

The use and deployment of AI system may give rise to liability for “the good, the bad and the ugly” use cases of AI.

Areas of potential liability

- Discrimination and bias
- Antitrust / competition
- Defamation
- Employment
- Data privacy
- Products liability
- Intellectual property liability / ownership
- Other civil liability / criminal?

Discrimination and bias

- One of the primary focuses of new laws and regulations
- Existing laws and regulations can and are being applied
- Training data is often biased, resulting in biased outputs
- Algorithmic coding also often reflects inherent biases in coders
- Bias can occur in various use cases, for example:
  - Employment screening and decisioning
  - Risk rating and rates

FORVIS

Data privacy

- Inadvertent or unlawful disclosures
  - Use of personal data in generative AI prompts without appropriate consent
- Unlawful data collection
  - Use of personal data for algorithmic training without consent
- Management of opt-outs and deletion requests
  - For automated decision making
  - For algorithmic training
  - Practicality of “how” with AI as a black box
- Data breaches

FORVIS

Intellectual property

- IP ownership of AI-generated outputs:
  - Potential loss of copyrightability for AI-generated works
  - Potential loss of patent protection for AI-generated inventions
  - In all cases, “some level” of human authorship or invention is required
- Infringement exposure
  - Training data exposure
  - General patent infringement exposure in any emerging technology
- Loss of trade secret protection
- Inadvertent disclosure of proprietary information

FORVIS

Hallucinations

- Outputs may or may not achieve the intended or desired result
- Outputs may be inconsistently accurate or inaccurate
- Like all systems, there is a need for audit and verification

FORVIS

Some examples – ChatGPT and Generative AI

- New York – Lawyers used ChatGPT to help write briefs for the court. ChatGPT included cites to cases that did not exist. The lawyers did not confirm the cites, and actually doubled-down on the results. The court stated that the lawyers acted in bad faith and conducted "acts of conscious avoidance and false and misleading statements to the court.“
- Georgia – Case against Open AI, as a result of false information provided by ChatGPT that the plaintiff embezzled money. The reporter that used ChatGPT backed checked the information and did not further distribute the information, but the defamation claim is still proceeding.

Both good examples of the importance of human oversight, and inherent risks of AI.

FORVIS

Some examples – discrimination and training data

- EEOC – Entered into a settlement with a company in which its software for interviewing and screening potential employees was programmed to exclude females over 55 and males over 60. This was a violation of the Age Discrimination in Employment Act (ADEA).

Employers need to understand, and are responsible for, the technology and AI used in their business.

- Training Data (Intellectual Property Claims) – A class action lawsuit filed in California in November 2022 is challenging that GitHub Copilot, which assists in writing computer code, improperly used certain training data; and Getty Images filed a lawsuit in the US in early 2023, following an earlier announcement in the UK, against Stability AI and Stable Diffusion contesting the appropriate use of images used to train the AI. The Recording Industry Association is also pursuing claims against AI companies related to the use of their members' music to train their models and products.

Highlights the challenges of large language models, and more specifically training data and the need to vet the permissions and appropriateness of its use.

FORVIS

FORVIS®

Enterprise governance

NAIC guidance

Principals of Artificial Intelligence (Published by the NAIC in 2020)

- Fairness and ethical use
- Accountability
- Compliance with state laws and regulation
- Transparency
- Safe, secure, fair and robust system

NAIC is only one framework. There are many others, including:

- GSA – AI Guide for Government
- Singapore – Model Artificial Intelligence Governance Framework
- Microsoft – Responsible AI
- NIST – AI Risk Management Framework

FORVIS

NAIC guidance

Laws and regulations apply regardless of methodology used to develop rates, rating rules and rating plans.

Insurer must ensure the use of the AI system does not result in unfair trade practices or unfair claims settlement practices.

Insurer must ensure that rates, rating rules, and rating plans developed using AI do not result in excessive, inadequate or unfairly discriminatory insurance rates.

It is the Insurer's responsibility for compliance – not a third-party vendor.

Conduct and use of AI systems is subject to investigation / review including market conduct actions.

FORVIS

NAIC guidance – AIS program

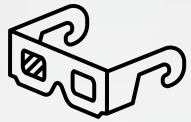
- Written program designed to assure decisions comply with applicable laws and standards
  - Assessment of risk posed by the AI system
  - Nature of decision being made
  - Potential harm to consumers
  - Extent to which humans are involved
  - Extent and scope of reliance on data and AI Systems from 3rd parties
  - Other factors?

- Three main areas:
  - Governance
  - Risk management controls and internal audit functions
  - Third party AI systems

FORVIS

NAIC guidance – AIS program

Requirements for AI corporate governance



Prioritize transparency, fairness and accountability

Cover the full AI system life cycle

Committee comprised of representatives from all relevant disciplines

Policies and framework approved by the Board / supervised by C-suite – executives

FORVIS

NAIC guidance – AIS program

- Risk management controls and internal audit functions
  - Document risk identification, mitigation, management framework and internal controls
  - Data practices (data lineage, quality, integrity, bias analysis, etc.)
  - Management of oversight of AI systems (documentation, measurements, benchmarking, evaluation for drift)
  - Testing and validation of AI system
  - Data and record retention
- Third party AI systems
  - Due diligence
  - Contractual terms
  - Audits and assessments

FORVIS

Regulatory and examiner review

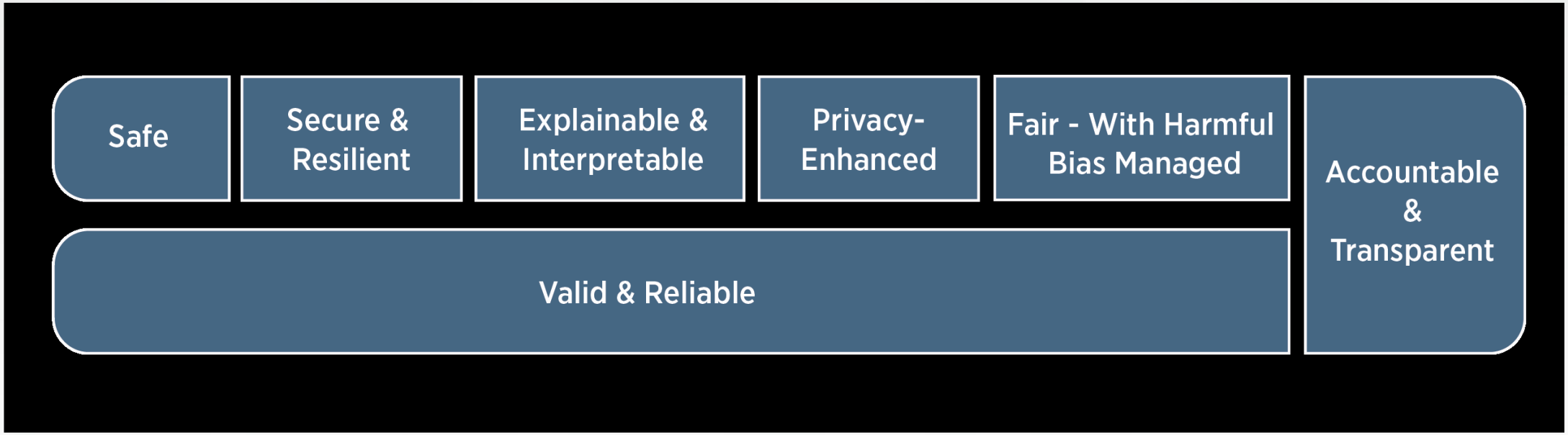
NAIC regulatory oversight and examination considerations

- What has the NAIC indicated will be required as part of an examination?:
  - Information and documentation on AIS program and application of AIS program
  - Information and documentation regarding evaluation of third-party AI system, contractual terms, and audit and confirmation of processes and terms

FORVIS

NIST AI Risk Management Framework

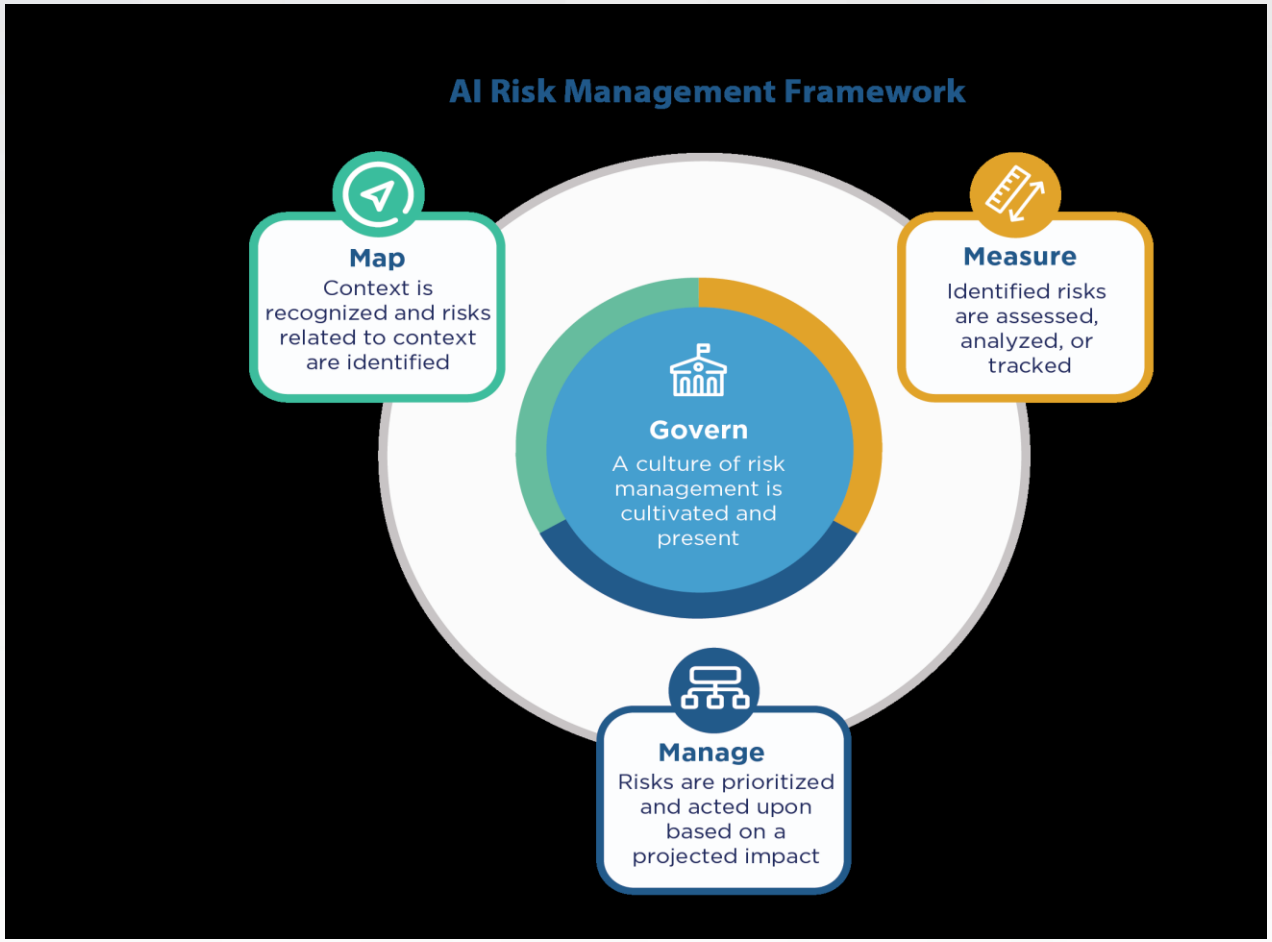
- Valid and reliable
- Safe
- Secure and resilient
- Accountable and transparent
- Explainable and interpretable
- Privacy-enhanced
- Fair – with harmful bias managed



From NIST AI RMF

FORVIS

NIST AI Risk Management Framework Core



From NIST AI RMF

FORVIS

NIST AI Risk Management Framework - Govern

- Policies, processes, procedures, and practices across organization related to the mapping, measuring, and managing of AI risks are in place, transparent, and implemented effectively
- Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping measuring, and managing AI risks
- Workforce diversity, equity, inclusion, and accessibility processes are prioritized in the mapping, measuring, and managing of AI risks throughout the lifecycle
- Organizational teams are committed to a culture that considers and communicates AI risk
- Processes are in place for robust engagement with relevant AI actors
- Policies and procedures are in place to address AI risks and benefits arising from third-party software and data and other supply chain issues

NIST AI Risk Management Framework - Map

- Context is established and understood
- Categorization of the AI system is performed
- AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood
- Risks and benefits are mapped for all components of the AI system including third-party software and data
- Impacts to individuals, groups, communities, organizations, and society are characteristics

NIST AI Risk Management Framework - Measure

- Appropriate methods and metrics are identified and applied
- AI systems are evaluated for trustworthy characteristics
- Mechanisms for tracking identified AI risks over time are in place
- Feedback about efficacy of measurement is gathered and assessed

NIST AI Risk Management Framework - Manage

- AI risks based on assessments and other analytical output from the **MAP** and **MEASURE** functions are prioritized, responded to, and managed
- Strategies to maximize AI benefits and minimize negative impacts are planned, prepared, implemented, documented, and informed by input from relevant AI actors
- AI risks and benefits from third-party entities are managed
- Risk treatments, including response and recovery, and communication plans for the identified and measured AI risks are documented and monitored regularly

Third party AI systems

Contracting from third party vendor

- Due diligence on the third parties, their data, models and AI systems
- Contracting terms specific for AI
  - IP rights in outputs and training/tuning of model
  - Right to use inputs to train model or limitations on same
  - Vendor monitoring rights/limitations
  - Compliance with laws and related risk coverage
  - IP infringement (broad enough to include data lineage issues)
  - Support of customer compliance obligations (ongoing monitoring, human oversight, opt-outs/deletions, etc.)
  - Data security and data privacy
  - Data sourcing (training data)
  - Expanded incident notification requirements (now cyber + model drift and similar issues)
  - Audit and examination rights (cooperation with regulators)
  - Confidentiality and disclosure obligations (model explainability)

See also – Society for Computers & Law (SCL) AI Group Artificial Intelligence Contractual Clauses

FORVIS

M&A activity

- Due diligence of the target's data, models and AI systems
- Third party contracts – are terms appropriate?
- Intellectual property and data privacy rights – ownership allocation, IP protections, use rights, etc.
- Suitability of AI developments and deployments – ethical, bias and discriminatory considerations

FORVIS

Questions?

forvis.com

FORVIS

Assurance / Tax / Advisory

nortonrosefulbright.com

Thank you!

forvis.com

FORVIS

Assurance / Tax / Consulting