

# cyberIdaho Financial Innovation Lab

## Emerging Technology Advisory Committee Report

### Artificial Intelligence Principles: A Technology Positive Approach

#### Executive Summary

Artificial Intelligence (AI) is here to stay in the financial services space, and a rational technology positive approach should be adopted that enables innovation to thrive for the benefit of society. AI presents many benefits and opportunities making it important to have a cautiously optimistic mindset to maximize its potential, while concurrently addressing issues as they arise.

A flexible non-prescriptive framework based on the principles found in this report is vital to responsibly maximizing the positive impacts of AI on society for the benefit of the public and financial industry.

#### AI Technology Innovation

1. **Workforce development is essential for building responsible AI solutions, systems, and regulation-** AI will touch everyone in some way, and the need to develop a workforce that understands how AI touches them (e.g., users, builders, deployers, or regulators etc.) is crucial. AI presents an opportunity to enhance the workforce but can also threaten elements of it. Training and education ought to be made available to the workforce to maximize the benefits of AI and mitigate potential worker displacement.
2. **Accessible data resources are necessary to enable small models to develop alongside large models-** Resources, structures, and mechanisms that help democratize training data will be important for a healthy AI ecosystem that enables small, medium, and large entities to flourish. Access to advanced computing resources in AI for smaller models is needed to enhance efficiency, drive innovation, and gain competitive advantages through data-driven insights and automation. Along with access to compute, there is a need for a robust open-source ecosystem that enables AI to develop transparently with public scrutiny.

#### AI Regulation

1. **AI standards ought to be flexible as the technology continues to evolve-** AI can't be perfect because humans are not perfect, which means we need to be flexible and agile in developing AI solutions and regulations making sure that innovation is not discouraged.
2. **Users should not have to be experts-** Subject matter experts in a specific discipline/domain shouldn't need to be experts in AI as well. AI tools must be continually evaluated for accuracy and there must be guardrails in place to provide quality control. Businesses should train employees on the safe and responsible use of AI, but controls are needed to make sure non-experts can use them.
3. **Transparency in data-** There must be transparency in training data, evaluation methods, results, etc., which can make users aware of potential biases in an AI system.
4. **Regulation should be focused on broad principles that foster competitiveness-** Placing substantial regulatory hurdles in front of small and medium enterprises before there is a strong understanding of AI behavior will harm competitiveness and provide larger enterprises with a regulatory capture advantage.

Taking enforcement actions that lead to prescriptive mandates will hinder innovation as society continues to learn and better understand AI for the purposes of developing smart regulation.

5. **AI safety regulation can only progress with the development of technical standards-** AI regulation without the development of technical standards will lead to uneven regulatory enforcement that will harm innovation. Creating measurable, repeatable, and objectively verifiable standards will take research, time, and experimentation. This means that AI safety will need to evolve as technical standards are created to strike the appropriate balance between public safety and innovation.

### **AI User Experience**

1. **AI should be viewed and used as a tool-** While futurists may exclaim the pending “AI Apocalypse”, AI in almost all current forms should be viewed as an assistant, not a replacement for repetitive human tasks and critical thought. A “human in the loop” approach should be adopted that leverages AI as a platform that can augment, rather than entirely replace, human effort and cognition. In the same fashion that any good carpenter “measures twice, to cut once,” users need to check the results of the tool, and not blindly trust in the accuracy of the tool.
2. **Explainability should not be a barrier to innovation-** Explainability shouldn’t be used as a barrier to innovation and goal achievement, but we should continue to work towards explainability. Technology development should not be hindered or slowed by explainability concerns. We must continue to foster innovation while preserving the ability to monitor results effectively and develop compliance tools to address accuracy.
3. **Private sensitive information should only become a part of AI models with consent-** AI systems should default to private and provide individuals/entities with control of their data/information. Businesses using AI should focus on responsible data stewardship that includes appropriate anonymizing of model data. Potential future privacy laws and policies could aid businesses in their development of privacy preserving AI models.

### **AI Compliance Risk Assessments**

1. **Cybersecurity for AI systems must be prioritized-** Across the cybersecurity threat surface area AI can be utilized to conduct cyberattacks, compromise systems, exploit vulnerabilities, and degrade capabilities. Cybersecurity – both defensive and offensive – must be a priority for any entity that relies on or uses AI tools.
2. **Enhance business enterprise risk management practices-** To mitigate unnecessary risk, businesses should implement AI platform security, as well as data security into measuring and managing enterprise risk. Leveraging robust accountability measures, businesses must define prohibited and acceptable AI practices and must develop/enhance risk assessment tools to address, and then monitor, these risks.
3. **AI system goals and results should be documented-** AI system goals should be clearly stated and documented to ensure algorithms are meeting desired outcomes. AI system results should also be documented and analyzed to determine potential adjustments and actions.
4. **AI tools must be monitored, maintained, and updated to maximize both innovation and safety-** AI is constantly evolving, which means frequent updates will be needed for maximizing innovation and safety.