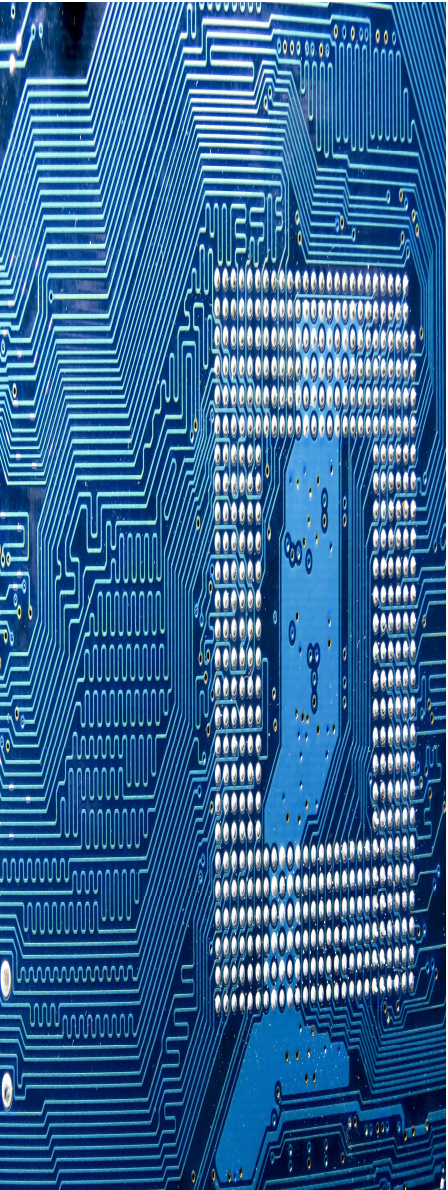


# A Practical Guide for Implementing an AI Risk Management Program

**An Introduction to a Series of Articles on AI Risk Management**

**Andrew Sommers, MBA, MSDS, JD**  
version 1.0 August 21, 2023



## Introduction

Companies should embrace and encourage the use of AI. Without the automated decision support and generative capabilities offered by AI, companies will fail to compete with their peers and startup competitors who will maximize the use of these tools. A company's exposure to AI will come from multiple sources including internal development, bespoke solutions developed by external parties, vendor provided systems, and reliance on third party service providers who make use of AI in their systems. When properly and safely implemented these tools improve products and services, create better customer experiences, and reduce costs. However, leveraging AI in systems comes with substantial risks.

This article is an introduction for a series of articles providing practical guidance for a company to implement a risk management program for the use of an AI algorithm, model, or component ('AI component') within a product, service, process, or system ('system').

While risk management is the focus of this series of articles, risk management should be viewed as a mechanism to encourage and facilitate the implementation of AI using guidelines to ensure a company has the necessary controls, documentation, and metrics to provide transparency to stakeholders about the risks and risk management of AI.

## Why Implement AI Risk Management?

Systems containing AI components can expose a company to many risks. The level of review and on-going monitoring of a system should be based on the level of potential risk from deployment and continued use. When assessing the potential risk of a system containing AI components, risks to consider include:

### Reputational Damage

A poorly managed AI implementation can negatively impact a company's reputation.

### Regulatory Compliance Failure

Regulations addressing AI risks have been introduced and more are expected.

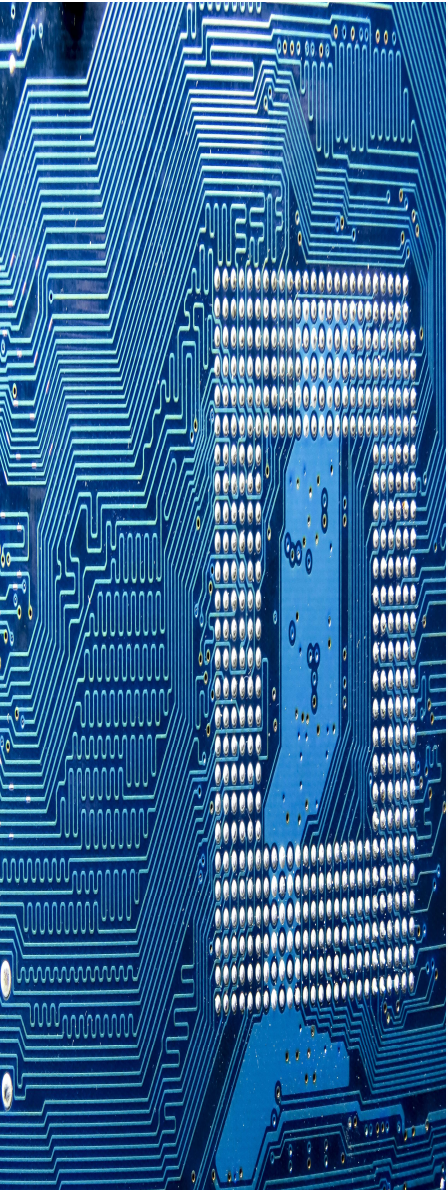
### Lost Sales and Profit Margins

Bad business decisions caused by poorly implemented AI can affect sales, profits, and margins.

### Private Legal Actions

A company may face legal action if an AI implementation infringes on individuals' rights.



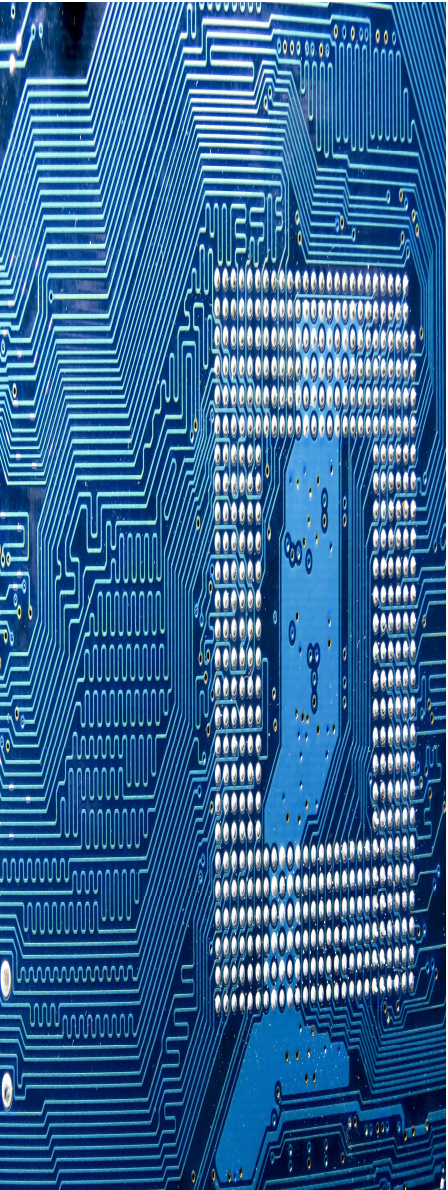


## Challenges When Implementing an AI Risk Management Program

To assist companies with managing the risks of leveraging AI, organizations including the National Institute of Standards and Technology ('NIST') and the Organization for Economic Co-operation and Development ('OECD') have developed frameworks to support 'Responsible AI', the implementation of controls to manage the risks and improve safety when embedding AI components into a system. These frameworks provide robust guidance on implementing AI risk management but are verbose and not highly prescriptive. Implementation of an AI risk management program based on these frameworks can be challenging.

Regulations to address the risks of AI have already been introduced, and the pace of new regulation will likely accelerate. Like data security and privacy regulations, the requirements are robust and complex. Implementation of controls to achieve regulatory compliance can also be challenging.

The classification of a component as AI can cause another source of complexity. Stakeholders will disagree on which components should be considered AI. The European Union's Artificial Intelligence Act<sup>1</sup> defines AI as, 'software that is developed with ... [machine learning approaches, logic- and knowledge-based approaches, and statistical approaches] and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with.' While the regulatory definition provides general guidance, a company managing the risks of deploying AI, including complying with regulations, requires a sufficiently inclusive but relatively simple method to determine which components, and therefore which systems, are within scope of its AI risk management program.

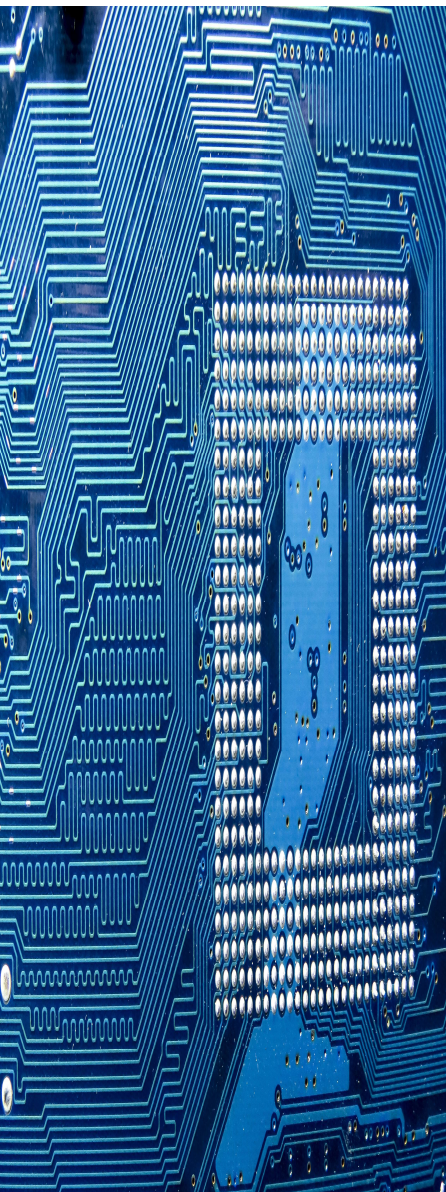


## A Series of Articles to Support Implementation of an AI Risk Management Program

The articles in this series will provide practical guidance for a company to implement a risk management program across the entire lifecycle of a system that includes one or more AI components. The series will follow the AI lifecycle stages of the NIST AI Risk Management Framework<sup>2</sup> but add an additional 'Decide' stage to provide guidance to support the initial decision on implementing an AI component or a system including AI.

Where a specific technical methodology is available to support the implementation of the AI risk management program for a specific stage in the AI lifecycle, a separate document on the methodology will be provided and referenced from the article for that lifecycle stage.





## Limitation of Scope

The series will discuss where the AI risk management program should ensure alignment with the company's data governance, security, and privacy programs. While data governance, security, and privacy are vital parts of managing the risk of systems that include an AI component, this series will not provide detailed guidance on these risk management functions. Other sources should be consulted for details of implementing these data and risk management functions.

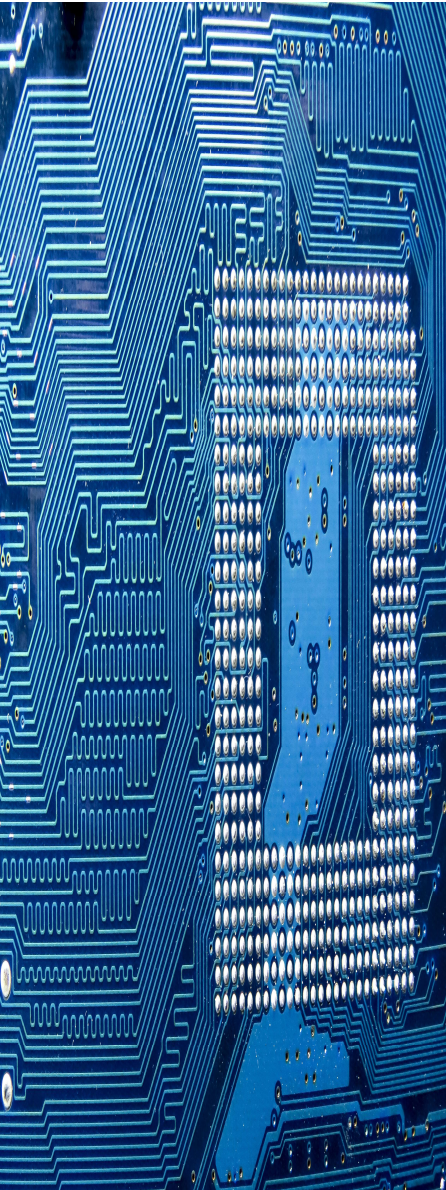
## Notes

The series is not and should not be used as legal advice or recommendations.

The articles provide practical guidance on developing an AI risk management program but should not be viewed as a comprehensive guide to AI risk and risk management and should be supplemented with other sources.

Articles might be updated from time to time to reflect updates to AI components, regulations, and risk management frameworks. See the version number and date on the initial page of this document.

This material is subject to copyright but available for public use. Please include the proper acknowledgement when referencing this document or any other articles in the series.



## References

- 1 European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence and Amending Certain Union Legislative Acts, April 21, 2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206>
- 2 National Institute of Standard and Technology, United States Department of Commerce, Artificial Intelligence Risk Management Framework (AI RMF 1.), January, 2023, <https://doi.org/10.6028/NIST.AI.100-1>
- 3 Images provided by pxfuel at <https://www.pxfuel.com/>