

Applying IT Governance Frameworks for Generative Artificial Intelligence

John Casamassa

Robert Morris University, United States
jjcst32@mail.rmu.edu

Wenli Wang, PhD

Robert Morris University, United States
wangw@rmu.edu

Abstract

Generative Artificial Intelligence (GAI) is a transformative force that organizations may have to embrace to remain competitive and safe. As organizations navigate the complexity of this new digital landscape, organizations seek appropriate governance frameworks to help balance the dual imperatives of harnessing GAI-enabled innovations and safeguarding against GAI-enabled cybersecurity threats.

The impact of generative AI on cybersecurity is a double-edged sword. This research discusses how hackers can take advantage of GAI to create realistic phishing emails with large language modelling, as well as how security professionals can apply GAI to generate synthetic data through reinforcement learning to fine tune AI models developed as countermeasures against phishing.

The research further introduces and compares relevant information technology (IT) governance frameworks for GAI. It identifies NIST AI RMF as the most suitable framework for managing risks unique to or exacerbated by GAI. It recommends COBIT 2019 for a large scope IT governance including GAI's goal alignment with organizational objectives and performance measurement for continuous improvement. It recommends NIST CSF 2.0 for its general process-based approach to address GAI-induced cybersecurity challenges. Both NIST AI RMF and NIST CSF2.0 were recently developed and updated in 2023 and 2024 respectively.

Overall, this research suggests organizations adopt multiple IT governance frameworks for a balanced approach to address the complexity in the new frontiers of generative AI.

Keywords: Artificial Intelligence, Generative AI, Governance, COBIT, NIST CSF, NIST AI RMF, Risk management