



Executive Training & Events for ERM Professionals

ERM PROFESSIONAL INSIGHTS

Capturing the Benefits While Managing the Risks of Generative AI Technologies

DON PAGACH

Professor of Accounting

Director of Research for the ERM Initiative

NC State University

Poole College of Management

Capturing the Benefits While Managing the Risks of Generative AI Technologies



DON PAGACH

Professor of Accounting
Director of Research, ERM Initiative
NC State University
Poole College of Management

Don Pagach is a professor of accounting and serves as the director of research for the ERM Initiative in the Poole College of Management where he helps lead our ongoing research related to ERM. Don has conducted extensive academic research that examines characteristics of organizations that implement enterprise risk management and how investors in the marketplace value the embrace by organizations of ERM processes. Currently he has ongoing research projects that examine the impact of integrating an organization's ERM processes with its focus on sustainability. Don also works closely with visiting PhD students who come to NC State to partner on research related to ERM. Don is one of the co-authors of the Initiative's annual survey report on the Executive Perspectives on Top Risks done in partnership with Protiviti.

The buzz surrounding the release of the latest artificial intelligence (AI) tools, such as OpenAI's ChatGPT has spanned the spectrum from something viewed as exponentially transformational, similar to the Industrial Revolution, to one that signals the end of the world. The strategic opportunities that these generative AI technologies may offer are mind-boggling while at the same time a bit scary. Business leaders are scratching their heads as they try to get their arms around how the tools might create competitive advantage for their organizations, without triggering out of control risks.

Proliferation of Generative AI Tools

Large language model tools, like ChatGPT and Google's Bard, reflect incredibly powerful technologies. Generative AI, such as Chat GPT and Bard, have been trained on huge datasets of text and software code that allow them to quickly respond to questions, with Chat GPT's strength being conversation and Bard's being research and education.

While Chat GPT and Bard have captured the most attention, other programs have been created to focus on more specific tasks, such as Amazon's CodeWhisperer that generates full functioning software code; Pi that serves as a personal assistant; and Replika, that focuses on building relationships as a companion. In addition, Meta (a/ka/ Facebook) has released its large language AI model, Llama 2, which has been trained on Meta's large set of data.

What's Different from Past AI Tools?

While these large language models that allow for communication have received significant attention over the past several months, AI technology and machine learning have been used for years by organizations. Google's Bard describes these two technologies in the following manner:

"Artificial intelligence (AI) is a broad term that refers to the ability of machines to perform tasks that are typically associated with human intelligence, such as learning and problem-solving. Machine learning (ML) is a subset of AI that focuses on the development of algorithms that can learn from data and improve their performance over time."

Calls for Pause in Embracing AI

What seems different today is the massive leap in capabilities with these latest releases. In some ways, "we don't know what we don't know." That has caused some - including AI experts - to call for a pause in development to examine the effect that AI and machine learning will have on education, industry and society at large. The Center for AI Safety (CAIS) has lobbied for a stop of AI development until the risks associated with AI are better understood. CAIS believes that the potential risks of AI result from the possible misuse of AI that could lead to disinformation and fake information. In addition, CAIS is concerned that the values of developers of AI systems may not be in alignment with human values and that AI systems could become so powerful that they become weaponized.

Become Risk Informed about Generative AI

Organizations are exploring all kinds of ways they may be able to leverage the tremendous advantages offered by these powerful tools. Executives are seeing the potential efficiencies

**CAPTURING THE BENEFITS WHILE
MANAGING THE RISKS OF GENERATIVE AI
TECHNOLOGIES**

Don Pagach

The existential risks of AI are underscored by the numerous operational risks that organizations are facing on a daily basis due to the use and development of products and services incorporating AI.

that might be available by using generative AI to do difficult and time-consuming tasks, such as conducting research on a topic or entity, reviewing and summarizing large contracts or other complex documents, or crafting proposed solutions to complex business problems. While the benefits can be eye-popping, it is important that business leaders not naively overlook potential risks that may far outweigh the return offered by AI.

Cautions When “Test Driving” Generative AI

In these early days of exploration, many business leaders might be “test driving” the generative AI capabilities by asking these tools to review critical documents and files to see how well the AI performs. But in doing so, they may be actually allowing their confidential documents to become part of the “public sources” AI uses to learn and improve. That means proprietary, confidential data has now exited the “walls” of the organization. Suddenly realizing this reality, many organizations are already creating boundaries within their IT platforms that prevent the use of open access generative AI platforms and only allowing the use of the tools within their platforms (and not on the open web). Blocking the use of generative AI tools that are not within the organization’s private IT systems may be an important first step to consider for your organization.

The existential risks of AI are underscored by the numerous operational risks that organizations are facing on a daily basis due to the use and development of products and services incorporating AI. Educational institutions are some of the first organizations to raise concern about the risks associated with AI as students use the new technology to write papers and complete research. However, underneath this is a concern about how AI will affect such things as curriculums, the job market for college graduates, the quality of learning and research and innovation.

Industries are also concerned about being able to compete against companies backed by AI systems, and they are focused on emerging regulatory compliance responsibilities, transparency of AI systems and how they might jeopardize confidential information, the cost of developing AI models and any liability that might arise from their use. For example, the use of AI programs might result in discrimination if the underlying data that is used to train the model contains bias. In addition, the use of AI is one of the main factors in the strike by the Screen Actors Guild where actors are concerned that AI can be used to replace numerous tasks such as voice-over work..

Embracing Best Practices Guidelines for Managing Generative AI Use

Given that the use of AI technology has quickly grown and more organizations are contemplating developing and using AI tools and programs, organizations are developing risk management frameworks to assess the risks associated with developing and deploying AI models.

The US Department of Commerce’s National Institute of Standards and Technology (NIST) recently released its [framework for AI](#) which was developed for organizations designing, developing, deploying, or using AI systems to identify and manage the risks of AI and promote trustworthy and responsible development and use of AI systems. The NIST’s framework contains four core functions to manage AI risk and develop reliable AI systems:

1. Govern
2. Map
3. Measure
4. Manage

At the core of the framework is **Governance** which requires putting in place the proper structures, systems, processes, and teams to ensure that risk management is embedded throughout the development, training and use of AI technology.

The **Map** function requires that development, training and use of AI be fully assessed. Because of the interconnections between these activities, and separation of developers, designers, and users it may be difficult to understand all of the risks associated with an AI model. The Map function should provide the AI organization with enough knowledge about the relevant risks in the entire AI model, from development to deployment.

CAPTURING THE BENEFITS WHILE
MANAGING THE RISKS OF GENERATIVE AI
TECHNOLOGIES

Don Pagach

*The "wow" of generative
AI must be balanced with
managing risks that accompany
the new opportunities that
evolving technologies offer.*


The **Measure** function requires that AI use qualitative and quantitative methods to track the risks identified in the MAP function. The framework suggests that “Measuring AI risks includes tracking metrics for trustworthy characteristics, social impact, and human-AI configurations.”

The final risk management function is **Management** of the AI system.

Staying Abreast

The speed at which the generative AI capabilities are being introduced is accelerating rapidly. While there is a “wow” aspect to these innovations, leaders of organizations will want to also pay attention to the risks introduced by these opportunities so that they can go in with their “eyes wide open” about the risks that need to be navigated. They don’t want the “new shiny object” to distract them from the realities unmanaged generative AI usage might present for their organization’s long-term success. Staying abreast of both the opportunities and risks offered by generative AI will ensure that the competitive advantages are realized without unexpected costs.

To learn more about navigating enterprise-wide risks in today’s rapidly changing business environment, visit our ERM Resources Center at www.erm.ncsu.edu.

<p>Visit Our ERM Online Resources</p> <p>ERM ARTICLE SUMMARIES https://erm.ncsu.edu/library/all-articles</p> <hr/> <p>ERM RESEARCH REPORTS https://erm.ncsu.edu/library/research</p> <hr/> <p>ERM VIDEO LIBRARY https://erm.ncsu.edu/library/video-insights</p> <hr/> <p>ERM PROFESSIONAL TRAINING & EVENTS https://erm.ncsu.edu/executive-education</p> <hr/> <p>SCM INDUSTRY PARTNERSHIPS http://scm.ncsu.edu/industry-partnerships/</p>	<p>Be 'In the Know'</p> <p>Get ERM articles, whitepapers, and research sent directly to your email inbox. Sign up online for our newsletter at HTTP://ERM.NCSU.EDU/</p>	<p>Contact ERM</p> <p>Poole College of Management, Enterprise Risk Management, NC State University 2801 Founders Drive Raleigh, NC 27695 919.513.0901</p> 
--	---	--