Swastik Singh

1315 NE Campus Pkwy Alder Hall 252

Seattle, Washington, 98105

swas@uw.edu

Artificial Intelligence in Enterprise Risk Management

Students use it to learn. Businesses are eager to implement it into their systems. Teams use it to cut costs and be more efficient. But what exactly is Artificial Intelligence (AI), and how can it help risk management professionals? AI is a beneficial tool that is becoming a necessity in fields like Enterprise Risk Management (ERM). AI comes with many benefits for businesses and teams, be it efficiency, accuracy, or costs. However, AI is not without risks and pitfalls.

Now, to get started, what is AI? AI is the ability of machines to mimic the functions associated with human intelligence, be it learning, reasoning, or problem-solving. AI also has various subfields, like machine learning, natural language processing, robotics, and computer vision. AI systems ingest a large amount of data to recognize patterns, make decisions, and improve as they receive more information.

What is Enterprise Risk Management (ERM)? As the fundamental focus of this course, INFO 312, ERM is defined as “the process by which organizations identify, assess, manage, and monitor risks to achieve their objectives.” ERM also has various domains, such as “operational, financial, reputational, strategic, and security risks.” Lastly, ERM has one major goal: to minimize “uncertainties through structured risk management strategies such as risk acceptance, mitigation, transfer, and avoidance”

But how does AI fit into ERM? According to KPMG, AI has been recognized for "its potential to significantly transform the day-to-day activities of a business" (Artificial Intelligence in Risk Management). But more specifically in ERM, "AI/ML has become synonymous with improving efficiency and productivity while reducing costs" (Artificial Intelligence in Risk Management). Despite the promise of AI, its integration into ERM isn't smooth. There are major concerns about data security, bias, and compliance with regulatory bodies. This paper is, in essence, a risk analysis on AI and how it can both impact the ERM landscape for good but also highlight the potential for negative impacts when it comes to AI.

Before going further, how can AI be used in ERM? What are some ways that have already been implemented? AI has been integrated into enterprise risk management to enhance decision-making, detect anomalies, and mitigate risks proactively. For example, in the finance industry, AI is used to analyze and "evaluate multiple risk factors simultaneously," (Hayes), allowing firms to identify vulnerabilities in trading and investment strategies. Aside from trading, banks use AI to do credit risk modeling. Banks use data to "process and train unsupervised learning algorithms," (Artificial Intelligence in Risk Management), assess the financial health of applicants, and predict default risks. Another thing that AI systems are excellent at is predictive analytics and anomaly detection. Both of these play major roles in "predicting credit card fraud." (Artificial Intelligence in Risk Management)

Beyond finance, AI is used in operational risk management across industries. For example, natural language processing (NLP) helps organizations process large amounts of unstructured data, such as compliance documents, news reports, and

regulatory filings, to identify emerging risks and trends. Beyond predictive analytics, AI also streamlines compliance monitoring through automation. Which leads to reducing manual effort and also minimizing human error. These tools benefit ERM by improving efficiency, reducing overhead costs, and enabling businesses to anticipate and respond to risks better.

A second major way AI is used in ERM is in risk identification and assessment. For example, AI is being used to enhance Anti-Money Laundering (AML) efforts. “Financial institutions utilize AI to scrutinize transaction patterns for suspicious activities.” (Srivastava) The goal of this is to accurately and efficiently detect issues so that the financial providers can do their due diligence and remain in compliance with regulatory bodies.

Aside from money laundering identification, AI is used in cybersecurity threat detection. AI systems are being “trained to monitor network traffic and spot unusual patterns that may indicate a breach.” (Srivastava) So, for example, if someone fails to log in to an account from a foreign IP address, the AI would notice, identify, and trigger security protocol or lock the account.

Another major example is in operational risk management, specifically in supply chain risk prediction. This is done by analyzing data “across the supply network to foresee potential bottlenecks.” (Srivastava) This could predict if a machine in a factory is close to breaking and prepare the factory managers to purchase or bring someone in to fix the machine.

These are only a few examples of risk identification. The logical next step after identification is risk monitoring and response. AI can be used as an “early indicator and

weak signal detection” (White) and “rapid geospatial orientation” (White), as well as to do “initial analysis and triage of potential event signals (at scale)” (White). This means AI streamlines complex processes. This allows smaller teams to handle the same workload as larger teams while maintaining the quality of work. Thus, AI reduces the need for multiple teams to manually assess risk into a much shorter process and effectively reduce costs for companies, which can then be used to focus on other risk areas.

There are many ways AI can benefit ERM, but it's highlighted in threat intelligence analysis, workplace risk reduction, and data classification, to name a few. AI is used in threat intelligence data that can be “analyzed at scale using machine learning engines and processed for likelihood calculations” (Shackleford) to create risk predictability models. This is vital in addressing issues like cloud account hijacking and ransomware infections in a timely fashion. In workplace risk reduction, AI can “analyze data related to workforce activities in high-risk environments” (Shackleford) to prevent accidents from being dangerous and potentially fatal. This will be done by leveraging AI to generate predictive predicaments and help improve safety measures. As for data classification and monitoring, AI can take current data and detect patterns to process, upload, and create a cloud environment to classify and tag new data. This would streamline processing and allow “compliance professionals to identify sensitive data that needs strong security protections.” (Shackleford) All these examples have a few things in common: they highlight the benefits of AI in improving efficiency and accuracy in risk assessments, enhancing predictive capabilities in early risk detection, automation of repetitive tasks, and aiding in data-driven decision-making.

While AI has benefits in ERM, it also carries many challenges, mainly in how data is being accessed and used, integration within legacy systems, cybersecurity within the AI models themselves, and human overreliance. First things first, AI is very susceptible to bias within data because of how they are developed. They are intended to identify patterns within data, and if those patterns have any sort of intrinsic bias, the AI algorithm will be “likely to amplify that bias and may produce outcomes that reinforce existing patterns of discrimination.” (Boillet) This can be highlighted at times when people file for credit scores at banks and also in hiring practices. Of course, the models themselves aren’t safe either. Mainly due to the cost of developing an AI model, managing AI will require 3rd party risk management practices. And because of that, malicious actors could target the AI developers to “steal personal data or confidential information about a company.” (Boillet) Lastly, human overreliance is a fundamental issue. This is because AI isn’t like a human; it is not good enough at understanding the data that it is working with, instead, it relies exclusively on its training data to provide insights. So, if their training data is biased, “their outcomes can be jeopardized” (Boillet) and impact the company in various ways, like legal risks and liabilities as well as reputational damages.

Because of these concerns, as AI becomes more incorporated into ERM, there needs to be strong governance to mitigate ethical, operational, and compliance risks. Many policies are being or have been enacted to promote “transparency, accountability, privacy, and fairness when developing and deploying AI tools.” (Bonnie) An example is Washington State House Bill 1168, which has been proposed during this cycle. On a global scale, using frameworks already in place, like the NIST AI Risk Management

Framework and the ISO AI Standards framework, would be extremely beneficial. To keep up with incoming regulations, security teams may need to implement policies that would involve defining acceptable AI use, approving AI apps, training personnel, and creating documentation related to AI development and use. On the operational side of things, AI models can struggle with performance decay where fraud detection models become less accurate and deal with sustainability issues like scaling and integrating the AI with current systems. These issues will impact the performance of the AI models and will slowly grow to impact the teams working with them. There needs to be a way to monitor and maintain those models. Lastly, humans need to be able to explain and justify their decisions. But an AI can not do that, it struggles to reason out why decisions are made. This stems from the way AI models behave; they act and respond according to their training data, but they can't reason out the choices for why doing one thing is better than the other. This shows a fundamental need for humans.

However, humans are unpredictable. Humans have different standards and risk appetites. That's why we need a way to standardize the human perspective. The best way to do that is by developing best practices, formulating ethical and governmental principles, and building resilient AI systems. Some of the ways ERM can use AI tools are getting the AI to do basic tasks like "draft reports and generating summaries of meetings" (Williams), "Research and data analysis to identify trends" (Williams), "support scenario analysis" (Williams), and "Bridging the gap from strictly qualitative assessment methods to quantitative" (Williams). The best practices also involve not using external AI tools to "connect risk information to strategic objectives." (Williams) This would protect private company data. For governance, risk managers need to be

aware of acts like the EU Artificial Intelligence Act that is “coming into effect in 2025” (Bonnie) and the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Both of which are coming in place “to develop standards for the safety, security, and testing of advanced AI models.” (Bonnie)

AI is an extremely promising tool in ERM, provided it is used well. It enhances accuracy, improves efficiency, and allows for proactive risk detection, all while having significant cost savings. AI can help streamline tasks, reduce human error, and boost organizational resilience, be it in predicting credit fraud, monitoring cybersecurity threats, or optimizing operational risk responses. However, AI still comes with risks: biased decision-making, third-party vulnerabilities, cybersecurity issues, and human overreliance. To address these issues, companies will need to build robust frameworks, follow regulatory compliance, and follow ethical guidelines as they monitor their AI systems. Ultimately, the best solution is to follow a hybrid model, one that balances AI’s capabilities and human oversight so that organizations can take full advantage of the tools at their disposal, managing risks, making informed decisions, and securing a competitive edge.

Works Cited

"Artificial Intelligence in Fraud Detection." *Wikipedia*, Wikimedia Foundation, 21 Oct. 2024, en.wikipedia.org/wiki/Artificial_intelligence_in_fraud_detection.

"Artificial Intelligence in Risk Management." *KPMG*, kpmg.com/ae/en/home/insights/2021/09/artificial-intelligence-in-risk-management.html. Accessed 13 Mar. 2025.

Badman, Annie. "Risk Management in AI." *IBM*, 30 Jan. 2025, www.ibm.com/think/insights/ai-risk-management.

Boillet, Jeanne. "Why Ai Is Both a Risk and a Way to Manage Risk." *EY*, MIT OpenCourseWare, 1 Apr. 2018, www.ey.com/en_gl/insights/assurance/why-ai-is-both-a-risk-and-a-way-to-manage-risk.

Bonnie, Emily. "Risk and Compliance in the Age of AI: Challenges and Opportunities." *Secureframe*, 25 Jan. 2024, secureframe.com/blog/ai-in-risk-and-compliance.

Chan, Bianca. "Here's How AWS Is Helping Financial Giants like JPMorgan and Bridgewater with Their AI Ambitions." *Business Insider*, Business Insider, 2 Mar. 2025, www.businessinsider.com/aws-wall-street-jpmorgan-bridgewater-mufg-rocket-mortgage-2025-2.

Chandler, Caitlin. "Inside the Black Box of Predictive Travel Surveillance." *Wired*, Conde Nast, 13 Jan. 2025, www.wired.com/story/inside-the-black-box-of-predictive-travel-surveillance/.

Colback, Lucy. “How We Can Use Ai to Create a Better Society.” *Financial Times*, 23 Jan. 2025, www.ft.com/content/33ed8ad0-f8ad-42ed-983a-54d5b9eb2d27.

“Data Analysis for Fraud Detection.” *Wikipedia*, Wikimedia Foundation, 3 Nov. 2024, en.wikipedia.org/wiki/Data_analysis_for_fraud_detection.

Datarails. “How Ai Can Help Enterprise Risk Management (ERM).” *Datarails*, 26 Aug. 2024, www.datarails.com/ai-can-help-enterprise-risk-management/.

“Ensemble Learning.” *Wikipedia*, Wikimedia Foundation, 28 Feb. 2025, en.wikipedia.org/wiki/Ensemble_learning.

Fulton, Richard, et al. “The Transformation Risk-Benefit Model of Artificial Intelligence: Balancing Risks and Benefits through Practical Solutions and Use Cases.” *arXiv.Org*, 11 Apr. 2024, arxiv.org/abs/2406.11863.

Brian Cassidy. “Applying Coso ERM Framework Principles to Ai.” *Deloitte United States*, 6 Sept. 2023, www2.deloitte.com/us/en/pages/audit/articles/applying-enterprise-risk-management-to-artificial-intelligence.html.

Hayes, Adam. “7 Unexpected Ways AI Can Transform Your Investment Strategy.” *Investopedia*, Investopedia, www.investopedia.com/using-ai-to-transform-investment-strategy-8778945. Accessed 13 Mar. 2025.

\Hightower, Satta Sarmah. “How One Texas-Based Moving Company Is Using AI to Improve Safety, Optimize Routing, and Reduce Liability.” *Business Insider*, Business Insider, www.businessinsider.com/texas-based-moving-company-uses-ai-to-boost-safety-efficiency-2025-2. Accessed 13 Mar. 2025.

Lambert, Yasmin. “In-House Lawyer Role Broadens in Response to Technological Change.” *Financial Times*, Financial Times, 10 Dec. 2024, www.ft.com/content/73e807cb-21fa-47a6-b934-0bb2439133b3.

Lingle, Brandon. “How Ai Is Working behind the Scenes at San Antonio’s Biggest Companies.” *News*, San Antonio Express-News, 20 Dec. 2024, www.expressnews.com/business/article/ai-use-san-antonio-companies-19468788.php.

McGee, Finlay. “Approaching Emergent Risks: An Exploratory Study into Artificial Intelligence Risk Management within Financial Organisations.” *arXiv.Org*, 8 Apr. 2024, arxiv.org/abs/2404.05847.

Murray, Seb. “Research Making a Real Difference.” *Financial Times*, 22 Jan. 2025, www.ft.com/content/2d017fa8-03db-4987-848a-8604ce5d67e4.

Ponick, Eva, and Gabriele Wieczorek. “Artificial Intelligence in Governance, Risk and Compliance: Results of a Study on Potentials for the Application of Artificial Intelligence (AI) in Governance, Risk and Compliance (GRC).” *arXiv.Org*, 8 May 2024, arxiv.org/abs/2212.03601.

“Predictive Analytics.” *Wikipedia*, Wikimedia Foundation, 13 Feb. 2025, en.wikipedia.org/wiki/Predictive_analytics.

Shackleford, Dave. “Ai in Risk Management: Top Benefits and Challenges Explained.” *Search Security*, TechTarget, 17 Nov. 2023, www.techtarget.com/searchsecurity/tip/The-benefits-of-using-AI-in-risk-management.

Srivastava, Sudeep. “Ai in Risk Management: Key Use Cases.” *Appinventiv*, 19 Feb. 2025, appinventiv.com/blog/ai-in-risk-management/.

Vartabedian, Mare. “AI Can Take the Slog Out of Compliance Work, but Executives Not Ready to Fully Trust It.” *The Wall Street Journal*, The Wall Street Journal, 17 Dec. 2024, www.wsj.com/articles/ai-can-take-the-slog-out-of-compliance-work-but-executives-not-ready-to-fully-trust-it-7cd60a16.

White, Kim. “How AI Will Shape the Future of Risk Management.” *Everbridge*, 23 Sept. 2024, www.everbridge.com/blog/how-centaur-ai-will-shape-the-future-of-risk-management/.

Williams, Carol. “Ai and ERM: Working Well Together to Build Competitive Advantage.” *Strategic Decision Solutions*, 30 May 2024, strategicdecisionsolutions.com/ai-and-erm-working-well-together/.