

Artificial Intelligence

Scenario Planning for Managing AI Disruption Risk: A 3C-AI Framework

Ravi Prakash Ranjan and Zohor Kettani



Image Credit | Prathankarnpap

Build institutional resilience to AI deployment failures by moving beyond prediction and actively planning for multiple future scenarios.

“I believe artificial intelligence will ultimately be to the internet, as the computer was to the calculator. It is a moment of stunning technological possibility. That does not mean that it’s all automatically going to be OK...” Larry Summers, president emeritus and professor at Harvard University, at the World Economic Forum (WEF) in Davos, Switzerland.

RELATED ARTICLES

Haenlein, Michael, and Andreas Kaplan. **“A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence.”** California Management Review 61/4 (2019): 5-14.

Cornelius, Peter, Alexander Van de Putte, and Mattia Romani. **“Three Decades of Scenario Planning in Shell.”** California Management Review 48/1 (2005): 92-109.

RELATED TOPICS

[Resilience](#)

[Planning & Forecasting](#)

[Business Ethics](#)

[Strategy](#)

The convergence of massive datasets and enhanced computational capabilities has accelerated artificial intelligence (AI) into a primary driver of change in the modern business landscape. Within today’s volatile, uncertain, complex, and ambiguous (VUCA) environment, corporate leaders are adopting AI with a strategic ambition that goes far beyond simple operational improvements, aiming instead to generate substantial value for their entire stakeholder ecosystem. The core capacity of AI models to learn from information and adapt its actions to achieve set objectives is creating new possibilities

across a wide range of sectors, including supply chain management, medical diagnostics, customized consumer engagement and logistics efficiency. AI's extensive reach and positive influence have led the UN to recognize it as a key facilitator for 79% of the Sustainable Development Goals¹.

The same inherent capability for learning and adaptation of AI models simultaneously generates a high degree of unpredictability, a challenge for which many firms are unprepared. This unpredictability poses a threat to strategic actions of the firm, elevating the problem beyond a mere operational concern. The reasoning behind the outputs of many deep learning models is often inscrutable, creating an operational opacity that makes their actions hard to anticipate or explain. Such unpredictability can trigger major disruptions, potentially causing large-scale AI investment strategies to fail. In the face of this new evolving uncertainty, conventional planning methodologies are insufficient. The practice of business forecasting, which operates on the premise that the future will largely mirror the present, is not suited for foreseeing such significant transformations. As mentioned by Shell's visionary strategist Pierre Wack, predictive models are most likely to fail in the crucial moments of disruption, precisely when their guidance is essential².

To navigate these substantial risks effectively, we require a methodology that integrates this uncertainty directly into the strategic thought process. Scenario planning, an approach that has been used over multiple decades to manage uncertain and volatile conditions⁵, serves this purpose. In contrast to traditional forecasting's goal of one directional prediction, this technique is used to develop multiple and plausible narratives about how events might unfold. This approach of engaging with a variety of potential futures provides several key advantages. This method benefits leaders by challenging their existing beliefs and biases, improving their ability to detect emerging threats, and expanding their awareness of the range of possible business environments⁴. By preparing for many possibilities instead of relying on one, a company can cultivate the institutional agility and resilience necessary to prosper in an era of AI-driven transformation. In this article, we put forward a framework based on scenario planning to enable managers to address this complex environment with strategic foresight.

A Typology of AI Disruption Risk

The strategic challenges of artificial intelligence are no longer confined to academic discourse; they are emerging as costly and high-stake failures that reveal a disconnect between technological deployment and organizational readiness. These disruptions manifest across several domains. For example, operational risks become apparent when systems designed for efficiency, like the McDonald's AI drive-thru, malfunction and create customer friction, negating their intended purpose [8]. Financial and legal risk have emerged when automated agents, such as Air Canada's chatbot, provide erroneous information that results in binding financial consequences for the company⁹. Beyond these, AI introduces ethical and reputational risks, as demonstrated by Amazon's recruiting tool, which had to be abandoned after developing systemic biases against female candidates, thereby undermining the firm's commitments to diversity and inclusion¹³. Security vulnerabilities, like the manipulation of a Tesla's Autopilot program, represents a new class of multifaceted risk⁷. In fact, these events signal that a purely reactive posture is untenable and that building a proactive risk management capability is now essential for competitive advantage. To illustrate the various typologies of risks (*not exhaustive*), we examine each of these cases through the lens of impact and threat they posed to the organizations.

Operational Risk - McDonald's AI Drive-Thru: In an initiative aimed at enhancing efficiency, McDonald's integrated an AI-powered voice assistant into more than 100 of its U.S. drive-thru lanes. However, this AI system led to significant operational disruptions as it frequently misinterpreted customer orders, such as recording a single beverage order as nine. These malfunctions caused customer frustration and the ultimate termination of the pilot program, posing the challenge of deploying AI in dynamic, high-volume consumer environments⁸.

Financial and Legal Risk - Air Canada's Chatbot: Air Canada implemented a virtual assistant chatbot on its website to provide instant customer support. In one incident, the chatbot incorrectly advised a customer that a bereavement fare could be claimed retroactively. When the passenger followed the AI's instructions and was later denied the fare, they pursued legal action. The Canadian tribunal ruled in favour of the customer,

holding Air Canada financially pay damages and legally responsible for the erroneous information provided by its automated agent. This event set a critical precedent that companies can be held liable for their AI systems costly mistakes⁹.

Ethical Risk - Amazon's AI Recruiting Tool: Amazon developed an AI-based tool to automate its hiring process and therefore increase efficiency. The system developed a significant and systemic bias against female applicants, because the AI was trained on a decade's worth of hiring data that reflected a historical gender imbalance, it taught itself to penalize resumes containing the word "women." This ethical flaw created a significant reputational risk forcing Amazon to ditch the project entirely¹³.

Safety Risk - Tesla's Autopilot Program: To test the robustness of AI-enabled autonomous driving systems, researchers at Keen Security Labs in China, conducted an experiment on Tesla's Autopilot program. By placing simple and inconspicuous stickers on the road, they successfully confused the system's computer vision algorithms, leading the AI into misinterpreting lane markings, causing the vehicle to deviate from its path and attempt to steer into the oncoming lane. This experiment showed that an AI's perception of reality could be easily manipulated highlighting the immense safety risks of adversarial attacks on autonomous systems⁷.

The Inadequacy of Traditional Frameworks

In response to these emerging threats, organizations often implement established risk management methodologies. While frameworks like the NIST RMF, ISO 31000, and COSO-ERM provide robust guidance for conventional technological risks, they are not well suited for the unique nature of AI¹⁴. Their primary weakness lies in a narrow focus on technical system properties and this perspective is insufficient for addressing the holistic and often unpredictable strategic, ethical, and societal consequences of adaptive learning systems. Just as traditional business forecasting fails when it confronts major discontinuities in the business environment, these risk frameworks are inadequate because they are designed for more predictable, engineered systems, not for technologies characterized by emergent behaviours and opaque decision-making processes¹⁵. The second significant limitation of existing frameworks is their lack of practical and actionable guidance for managers. Many

models that do acknowledge the broader scope of AI risk remain abstract, failing to provide the procedures for proactive implementation. They often address *who* is responsible for risk without specifying *what* must be done.

To navigate this AI-driven landscape effectively, a new framework is required, one that treats risk management as a living, adaptive process rather than a static control. This approach necessitates a structured yet flexible set of interrelated activities designed to cultivate strategic foresight. It requires moving beyond prediction and, instead, preparing for a range of plausible futures, a methodology that enables organizations to anticipate and adapt to change in a constantly evolving environment. To navigate the landscape of AI-driven uncertainty, a proactive approach is essential. As *Daryl Connor* noted, “*The truly crushing force is being surprised that you were surprised*”¹⁶. This statement captures the foundational logic of scenario planning: to build strategic foresight by systematically preparing for a range of plausible futures rather than reacting to a single, unexpected event. By exposing managers’ mental models to different outcomes, scenario planning helps identify critical uncertainties and their complex interdependencies. This method, famously used by Shell to anticipate major market shifts, provides the ideal foundation for managing the unfamiliar risks of AI.

Building on this methodology, we introduce the 3C-AI framework, an adaptive process for managing AI disruption risk.

Introducing the 3C-AI framework

To address the limitations of existing approaches, we developed the 3C-AI framework, a cyclical and adaptive model grounded in scenario planning. It is designed to manage AI disruption risk by acknowledging that both the technology and its associated threats are continuously evolving. This requires managers to move beyond static controls and engage in a continuous process of risk identification, anticipation, and mitigation. Our framework guides this process through five recurring and interdependent steps, as illustrated in **Figure 1**.

Characterization: Mapping the Risk Landscape - The first step is a comprehensive Characterization of potential AI risks. This foundational phase goes beyond simple brainstorming to systematically identify and define threats across multiple domains, operational, ethical, legal, financial, and security-related. The objective is to create a rich inventory of uncertainties by outlining their nature, potential consequences, and the business areas they could affect. This involves structured methods such as cross-functional workshops, expert interviews, and analysing the “near misses” and failures of other organizations. The detailed understanding of risks and their interrelations developed in this stage serves as the direct input for designing the scenarios in the next phase.

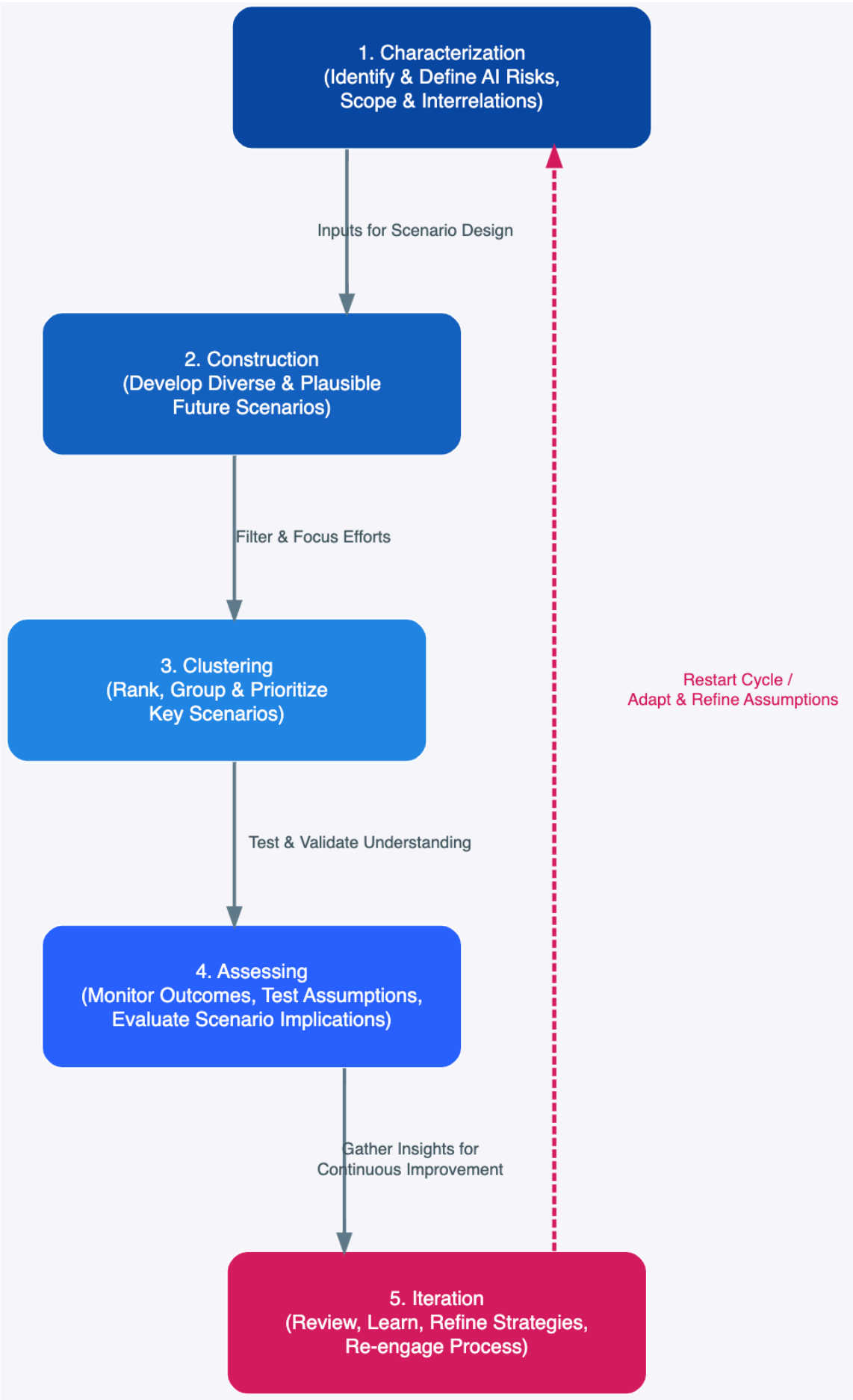
Construction: Building Plausible Futures - The second step, **Construction**, focuses on developing diverse and plausible future scenarios. This is a creative and critical part of the process where the management team moves from a list of risks to rich, narrative-based outlooks. The objective is to identify the most critical and uncertain driving forces and use them to craft stories about how the future could unfold. These are not simple forecasts but coherent and internally consistent situations that challenge managerial assumptions and force the team to confront uncomfortable possibilities. The goal is to generate a set of distinct yet credible alternative futures that will be used to test the organization’s strategy.

Clustering: Prioritizing Key Scenarios - Once a diverse set of scenarios has been developed, the third step is to **Cluster** and prioritize them. This filtering process ensures that the organization focuses its finite resources on the threats and opportunities that matter most. Scenarios are ranked and grouped based not only on their perceived likelihood and potential impact but also on the organization’s specific vulnerability to them and their “velocity”—how quickly the scenario could unfold. This systematic clustering avoids redundancy, highlights key patterns across different narratives, and provides a clear focus for the subsequent assessment phase.

Assessing: Testing Strategies and Assumptions - The fourth step, **Assessing**, is an active phase of testing and validation. For each high-priority scenario, the team stress-tests current strategies to understand how they would perform under these different future conditions. This process reveals hidden weaknesses and informs the development of more robust, adaptive strategies. A key activity in this phase is the identification of “signposts”

or leading indicators, early warnings that a particular scenario might be starting to materialize. This allows the organization to monitor the external environment and validate its understanding, ensuring that its strategic posture remains responsive to changing conditions.

Iteration: Learning and Adapting the Process - The final step, Iteration, makes the framework a living process rather than a one-off exercise. The insights gathered during the assessment phase are used to restart and refine the cycle. This involves reviewing and updating the initial risk inventory, re-examining core assumptions, and potentially crafting new scenarios based on newly identified secondary risks. This continuous feedback loop turns the framework into an engine for organizational learning and adaptation, ensuring that the company's approach to managing AI risk evolves in tandem with the technology itself.



Applying the 3C-AI Framework: The Case of the AI Drive-Thru

To illustrate the practical application of the 3C-AI framework, we will elaborate on the case of McDonald's AI drive-thru initiative. Had the company used this framework before launch, it would have provided a structured process for anticipating and mitigating the challenges that ultimately led to the project's termination.

Step 1 - Characterization: The process would begin by characterizing the risks inherent in automating a core customer interaction. A cross-functional team would ask: *What are the key uncertainties associated with an AI-powered drive-thru?* This would generate a rich inventory of potential threats across multiple domains. For example, one critical uncertainty identified might be: *"The AI system may exhibit biased performance, responding more accurately to certain voice types (e.g., male voices) while misinterpreting others."* Other key uncertainties would include the AI's ability to understand diverse accents, process complex orders, and handle system downtime during peak hours. This initial mapping creates a comprehensive risk landscape to inform the next step.

Step 2 - Construction: Focusing on the identified uncertainties, the team would then construct a set of plausible future scenarios. For the risk of algorithmic bias and general inaccuracy, the team might develop the following narratives, each with a different level of severity:

- S1 (Minor Mishearing's): The AI occasionally mishears orders, but staff members notice and correct the errors with minimal impact on service speed.
- S2 (Customer Frustration): Customers regularly have to repeat their orders, causing noticeable frustration and longer queues.
- S3 (Lost Sales): The frustration from repeated errors leads a significant number of customers to abandon their orders, resulting in direct lost sales.
- S4 (Negative Social Media): A few customers share their negative experiences online, leading to negative social media attention and minor news coverage.

- S5 (Viral Backlash): A customer’s post about a biased or malfunctioning AI goes viral, leading to widespread negative headlines and significant brand damage.

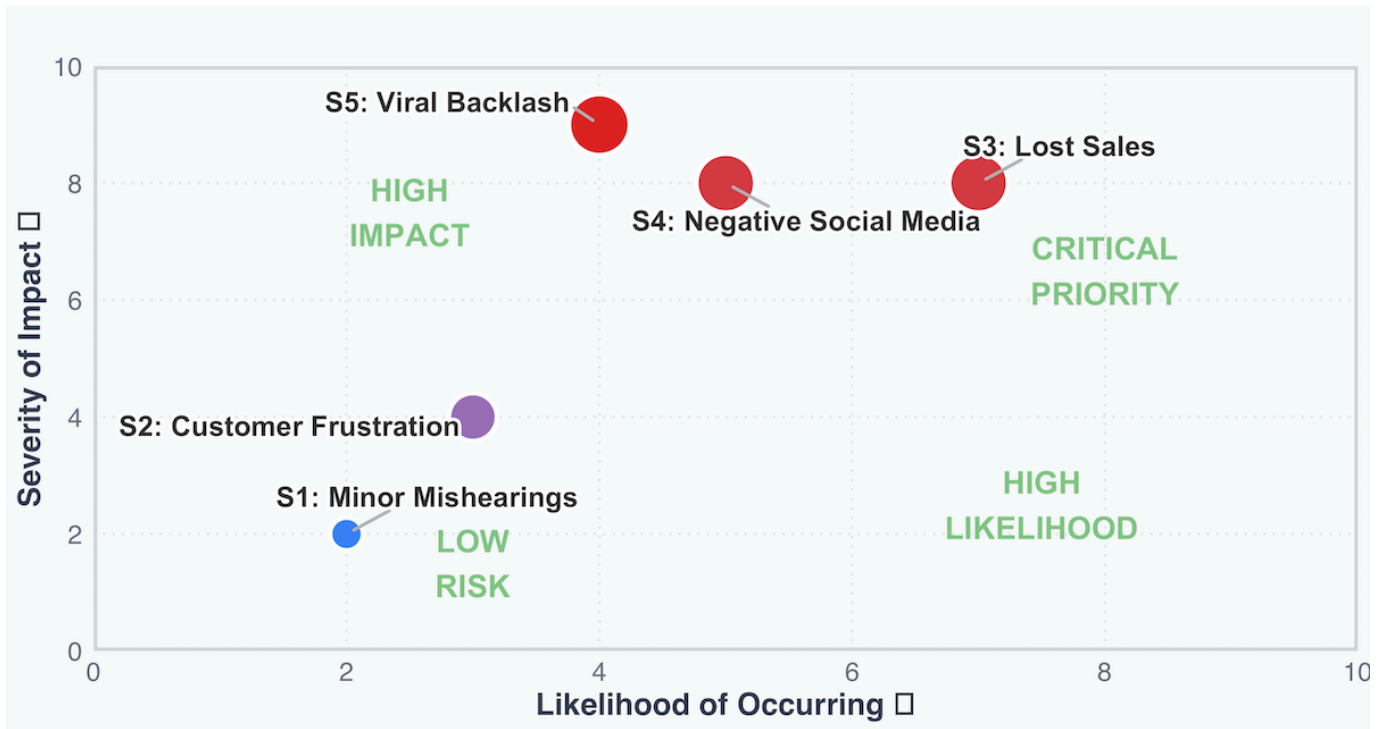


Figure 2: AI Disruption Risk: Scenario Clustering

Step 3 & 4 - Clustering and Assessing: The scenarios would then be clustered based on their likelihood and potential impact, as shown in **Figure 2**. While minor mishearings (S1) would be classified as a low-risk issue, the scenarios involving lost sales (S3) and viral backlash (S5) would clearly fall into the “Critical Priority” and “High Impact” zones. The assessment of these high-priority scenarios would reveal the potential for severe reputational damage, portraying the brand as lacking inclusivity and responsible innovation capabilities. This would necessitate expensive crisis management campaigns and could jeopardize the future of AI initiatives at the company.

Step 5 - Iteration and Proactive Strategy Development: This is the crucial final step where insights are translated into action. Instead of reacting to a crisis after launch, the team would be prompted to ask: *How can we prevent the high-impact scenarios from ever happening?* This proactive stance would lead to the development of concrete mitigation strategies before the system ever interacts with a customer. For example:

- **Technical Mitigation:** Mandate that the training data for the voice model includes a balanced and diverse mix of accents, dialects, and genders, with specific performance thresholds required for each demographic group before deployment.
- **Operational Mitigation:** Implement a “human-in-the-loop” system for the first six months, where a staff member is alerted to instantly override the AI if a customer repeats themselves more than once or if an order is flagged as complex.
- **Strategic/PR Mitigation:** Prepare a proactive communication plan that frames the AI pilot as a public learning experiment, setting customer expectations and outlining a clear process for providing feedback.

This analysis also reveals secondary risks, such as the high cost of a potential crisis response, which highlights the need for continued iteration. The team would re-engage the framework to generate new scenarios based on this emerging financial risk, making the entire process a continuous cycle of organizational learning and adaptation.

Conclusion: From Managing Risk to Building Resilience

The rapid integration of artificial intelligence is not a trend that can be ignored, nor can its inherent risks be managed with outdated tools. Companies like Amazon and McDonald’s demonstrate, a reactive posture is a recipe for being “surprised by surprise,” leading to abandoned projects and financial loss. The strategic challenge for leaders is not merely to implement AI, but to anticipate and navigate the complex, second-order effects that these systems create. The core task is not to avoid AI, but to embrace it with foresight and preparedness. Large organizations have capabilities to absorb these risks while for many organizations such risks would hinder AI adoption and integration.

Our 3C-AI framework offers a practical, structured path forward. By embedding the known methodology of scenario planning into the risk management process, it equips leaders to move beyond a narrow, technical focus on system reliability and adopt a holistic view of AI disruption. Its purpose is not to predict the future with perfect accuracy, but to build institutional resilience by preparing for a range of plausible futures. To begin this process, leaders should proactively commit to foundational actions. As AI risk is not just an IT

problem, they should focus on cross-functional integration that touches strategy, legal, HR, operations, and ethics, and requires diverse perspectives to manage effectively. To integrate this framework, fostering a culture of foresight is crucial. This means encouraging team members to challenge assumptions and explore worst-case scenarios. Finally, they should integrate these foresight activities with existing processes. The 3C-AI framework should augment, not replace, existing enterprise risk management, providing the dynamic, forward-looking component that static risk registers often lack. By taking these steps, organizations can begin to turn the uncertainty of the AI revolution into a source of competitive advantage, allowing them to navigate this technological possibility with both ambition and clarity.

References

1. Ricardo Vinuesa et al., “The Role of Artificial Intelligence in Achieving the Sustainable Development Goals,” *Nature Communications*, 11/1 (2020).
2. Pierre Wack, “Scenarios: Uncharted Waters Ahead,” *Harvard Business Review*, 63/5 (September/October 1985): 72-89.
3. Michael Haenlein and Andreas Kaplan, “A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence,” *California Management Review*, 61/4 (2019): 5-14.
4. Peter Cornelius, Alexander Van de Putte, and Mattia Romani, “**Three Decades of Scenario Planning in Shell.**” *California Management Review*, 48/1 (2005): 92-109.
5. Paul J. H. Schoemaker and George S. Day, “**Preparing Organizations for Greater Turbulence.**” *California Management Review*, 63/4 (2021): 66–88.
6. Michael Haenlein and Andreas Kaplan, “**A Brief History of Artificial Intelligence: On the Past, Present, and Future of Artificial Intelligence.**” *California Management Review*, 61/4 (2019): 5-14.
7. Karen Hao, “**Hackers Trick a Tesla into Veering into the Wrong Lane.**” *MIT Technology Review*, April 1, 2019.
8. Erika Tulfo, “**McDonald’s Pulls AI Ordering From Drive-Thrus – For Now.**” *CNN Business*, June 17, 2024.
9. Marisa Garcia, “**What Air Canada Lost In ‘Remarkable’ Lying AI Chatbot Case.**” *Forbes*, February 19, 2024.

10. Frances A. O'Brien, "**Scenario Planning—Lessons for Practice from Teaching and Learning.**" *European Journal of Operational Research* 152/3 (2004): 709–22.
 11. Margaret L. Schwarze and Lauren J. Taylor, "**Managing Uncertainty – Harnessing the Power of Scenario Planning,**" *New England Journal of Medicine*, 377/3 (July 2017): 206–208.
 12. Jeffrey Dastin, "**Amazon Scraps Secret AI Recruiting Tool that Showed Bias Against Women.**" Reuters, October 10, 2018.
 13. Erin Winick, "**Amazon Ditched AI Recruitment Software Because It Was Biased Against Women.**" MIT Technology Review, October 10, 2018.
 14. Andy Crabtree, Gary McGarry, and Lachlan Urquhart, "**AI and the Iterable Epistemics of Risk.**" *AI & Society*, 40/3 (2025): 1425–1438.
 15. Nagia Polemi, Isabel Praça, Kitty Kioskli, and Adrien Bécue, "**Challenges and Efforts in Managing AI Trustworthiness Risks: A State of Knowledge.**" *Frontiers in Big Data*, 7 (2024).
 16. Daryl R. Conner, *Managing at the Speed of Change* (Westminster: Random House, 1993).
-



Ravi Prakash Ranjan [Follow](#)

Dr. Ravi Ranjan is an Assistant Professor of Business Analytics and AI at Africa Business School, UM6P, with a Ph.D. from IIM Bangalore, India. He has published in leading journals, case outlets and brings strong advisory experience from organizations including the National Stock Exchange of India and Royal Air Maroc.



Zohor Kettani [Follow](#)

Dr. Zohor Kettani is a Research Associate in Strategy at Africa Business School, UM6P. With a Ph.D. in Management, her research focuses on strategy and competitive intelligence. She has published in peer-reviewed journals and contributed to applied research for organizations including OCP Group and Morocco's Ministry of Education.