Grant Thornton

Navigating AI Governance, Risk, and Compliance

Teaser Video Transcript

AI principals

While AI is certainly not new, IT has undergone this significant shift and the barrier to adoption is much lower than it was for decades. With this, we are seeing traditional governance frameworks being disrupted as generative AI has unlocked new capabilities like content generation, reasoning, and autonomous decision making. So as such, we've seen over the last two years organizations adopting new frameworks to support them on their AI transformation journey. Looking to legal frameworks like the EUAI Act or standards like the NIST Risk Management Framework, ISO 42,001, organizations are enshrining a set of principles to guide them.

And while Derek mentioned that there is no set as AI specific federal law in the US, existing laws for equal opportunity, fair lending, and deceptive trade do apply. And these are considerations that organizations are taking into account as they develop their principles and policies. So while each organization has their own distinct considerations to account for like industry, technological maturity, tech talent, region of operation, and overall organizational risk tolerance, they are enshrining these principles into their policies to guide adoption and development. Fairness helps to guide our practices. So they are not harboring bias, right? These systems tend to amplify existing biases that are hidden within the data that we have.

So if we don't have representative data in individual 1 to 1 engagements, now we have a system that is going to amplify that existing bias. Transparency ensures that we are open about how our systems work. They outline the data that is processed, the logic behind the algorithm, and the overall impact of an AI system on an individual. These are all essential for both users and people who may be impacted by these systems. Privacy and security mandate accountable use and responsible management, safeguarding data in AI systems. Inclusivity ensures that we are developing systems that foster inclusivity and growth for all. Not just for users, but we have to think about all of individuals who may be impacted within the context of a deployment, right?

AI poses unique risks

So now that you know Derek and Bex have really covered the foundational steps for building an AIGRC program, it's crucial to understand why this foundation is necessary, right? So AI brings with it a unique set of risks that requires specific attention and proactive governance for organizations. So as you can see on the side, right, these risks are not just limited to technical challenges. They extend to ethical, legal, operational, and reputational concerns. So briefly going over some of these risks, right? So first, bias. So AI models can reinforce societal biases if trained on incomplete or skewed data, which can lead to unfair or discriminatory outcomes.

Next on our list, we have privacy, right? So AI systems often handle personal data. There are growing concerns around consent, data protection, and the potential misuse of data. Another risk that AI brings is ownership. So the use of AI complicates questions of ownership and responsibility, especially when third party tools or data sets are involved. And then following that, we have explain ability. So many AI models operate as those quote UN quote black boxes, right? And so that makes it difficult to understand, explain or even audit their decision making processes. And then there's of course, security as a risk, right? So AI systems are often susceptible to novel threats like adversarial attacks or even data poisoning. And then finally, a big one, right, regulatory compliance. So as AI regulations are continuing to evolve, staying compliant is critical to avoid legal and financial risks, as well as to protect the organization's reputation.