The AI chatbot, ChatGPT, is a LLM that you may have had bank employees ask to use at your institutions, and it may be one that you use yourself. With Artificial Intelligence (AI) being built into Windows, Office, Adobe Acrobat, and web browsers and bank employees possibly using ChatGPT in the course of their daily tasks, it is essential for banks to implement controls, update risk assessments, and make enhancements to policies to help protect from the risks that AI poses.

To help you understand and manage the potential risks from AI, we recommend the OWASP Top 10 for LLMs (large language model). This list, which identifies the most critical vulnerabilities found in applications utilizing LLMs, is a practical and actionable resource. It's designed to provide security experts with concise security guidance that can be applied to navigate the complex and evolving terrain of LLM security, ensuring you're well-prepared to handle AI risks.

If you need assistance familiarizing yourself with some of the risks associated with AI, or if you're ready to start developing controls and updating your risk assessments, you can start by checking out OWASP's Top 10 **here.**

Contact CCI for guidance on updating policies and risk assessments at inquiries@completecompli.com.