ADVANCED CYBER SECURITY CENTER

Trusted Networks. Advancing Cyber Strategies.

AI Vendor Assessment Toolkit

Produced for CISOs, their Senior Staff making technology decisions, Risk Officers, and Legal Counsel. The following questions cover assessment of the 3 key elements of AI: data, computing power, and algorithms.

1. **Opportunities & management**
   a) What are your primary AI use cases and which specific AI technologies do you use?
   b) Can you provide references or case studies from clients in a similar industry or with similar AI needs?
   c) How are you enabling human oversight and collaboration for your AI systems?

2. **Evaluation**
   a) What kind of data does your AI system use for learning and how is it sourced, collected, prepared, and protected?
   b) What algorithms and models do you use, and how do you update them?
   c) How are you measuring AI tool performance and accuracy, including failures and errors, false positives and false negatives?
   d) How do you ensure accountability, transparency, and fairness in AI decision-making?

3. **Compliance with standards & regulations**
   a) What is your data retention policy, and how do you handle data now and after the engagement ends?
   b) How are you ensuring compliance with relevant AI ethics guidelines and regulations?
   c) How do you handle intellectual property rights concerning AI models and algorithms?
   d) How do you align with 3rd party risk management?

4. **Security & resilience**
   a) What is your disaster recovery plan for AI systems?
   b) How does your system adapt to new, unknown threats?
   c) How does your AI system protect itself from potential manipulation or tampering?

5. **Liabilities & protections**
   a) As a vendor, what steps have you taken to protect your company from potential liabilities associated with the use of AI?
   b) What steps have you taken to protect us from potential liabilities associated with the use of AI?
   c) Do you have insurance that protects your exposure and our exposure for AI tools, data, and IP?

ACSC AI Resources

AI Overview Slides, 2023 Annual Conference Marc Zissman, MIT Lincoln Laboratory	The AI Juggernaut, 2023 Annual Conference Briefing Summary ACSC Briefing Summary	CISA Roadmap for Artificial Intelligence Department of Homeland Security	Responsible Artificial Intelligence (RAI) Toolkit and Shield Assessment Department of Defense CDAO