CYBERSECURITY CONSULTING

AI Security & Governance

Independent governance and risk assessment for AI and generative-AI systems, policy, threat and risk assessment, and controls, before and after they touch sensitive data.

AI introduces new categories of risk: data leakage, prompt injection, model and output integrity, opaque decision-making, and fast-moving regulatory exposure. CyberX One helps you adopt AI responsibly with acceptable-use and governance policy, an AI-specific threat and risk assessment, and a controls framework mapped to emerging standards such as the NIST AI Risk Management Framework and ISO/IEC 42001.

Objectives

- Establish an AI acceptable-use and governance policy aligned to your risk appetite.
- Identify and rate AI-specific threats, data exposure, prompt injection, model and output integrity, third-party model risk.
- Ensure sensitive and personal data is handled lawfully across AI pipelines.
- Map controls to the NIST AI RMF and ISO/IEC 42001 and define human oversight.
- Prepare for emerging AI regulation before it becomes an obligation.

Outcomes & benefits

- **Responsible adoption**, a clear policy that lets teams use AI safely.
- **Risk visibility**, AI-specific threats identified, rated, and prioritized.
- **Data protection**, privacy obligations (PHIPA, PIPEDA, GDPR) addressed in AI workflows.
- **Controls assurance**, a defensible mapping to recognized AI frameworks.
- **Oversight**, monitoring, logging, and human-in-the-loop where it matters.

Scope of service

- Review of AI and LLM use cases, data flows, and pipeline architecture.
- AI threat and risk assessment following HTRA principles adapted for AI systems.
- Draft or refine your AI acceptable-use and governance policy.
- Controls mapping to the NIST AI RMF and ISO/IEC 42001, with a gap analysis.
- Recommendations for monitoring, logging, and human oversight of AI decisions.

Our process

1. **Discover**
   Inventory AI use cases, data flows, and the sensitivity of data involved.
2. **Assess**
   Run the AI threat and risk assessment and map controls to frameworks.
3. **Govern**
   Establish acceptable-use and governance policy with oversight controls.
4. **Remediate**
   Deliver a gap analysis and prioritized roadmap to close AI risks.

What you receive

- AI acceptable-use and governance policy
- AI threat and risk assessment report
- Controls mapping and gap analysis (NIST AI RMF, ISO/IEC 42001)
- Prioritized AI risk remediation roadmap

Engagement at a glance

TYPICAL DURATION	LED BY	SERVICE TYPE
~3-4 weeks	Cybersecurity Consultant	Assessment & advisory

NIST AI RMF · ISO/IEC 42001 · NIST CSF · PHIPA / PIPEDA

Ready to start?

Email **shah@cyberxone.ca** · **LinkedIn**

CyberX One Inc. · Markham, Ontario · Serving Canada

Book a discovery call