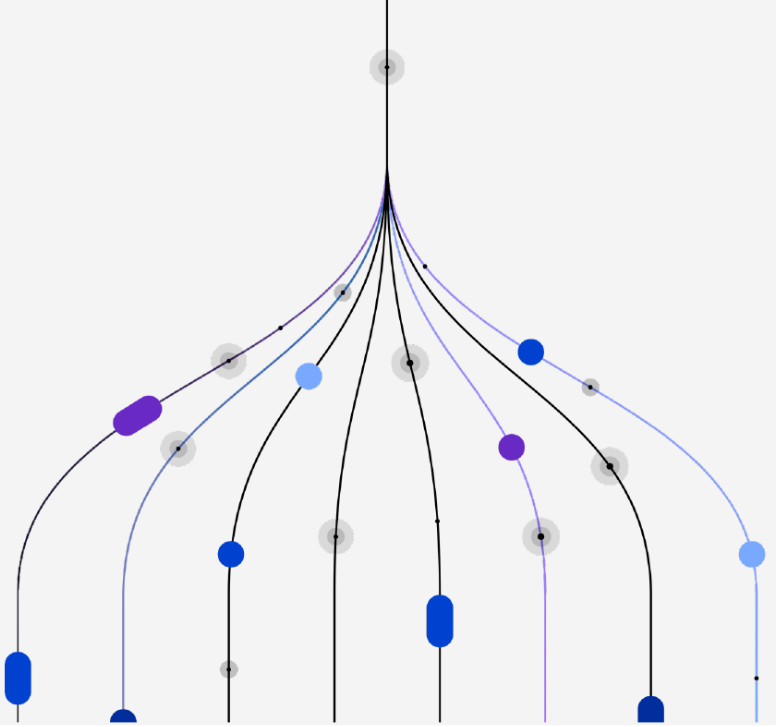
IBM **Technology Expert Labs**

Security Assessment Workshop for Gen AI

Safeguard your Generative AI environment and applications, enhance trust and transparency, ensure your data is protected, and empower your employees to focus on innovation, in a secure Generative AI environment.



Business Drivers

Generative AI (Gen AI) technology enables a completely new paradigm for rapidly making accurate business decisions, but it brings with it security challenges. Malicious actors may exploit vulnerabilities in insecure AI components, exploiting backdoors, introducing malware, or other malicious code into the system, and potentially leading to data breaches, system compromises, or unauthorised access.

By proactively addressing security concerns with Gen AI applications, organizations can demonstrate a commitment to responsible AI development and deployment, and foster trust with stakeholders, including customers, partners, and regulators.

Offering Highlights

Ultimately, securing Gen AI means identifying risks, implementing appropriate mitigations, and monitoring for issues. IBM Technology Expert Labs has pre-packaged a curated set of techniques, tools and architectures that support secure Gen AI applications within your enterprise.

Our workshop comprises an open a conversation between your team and IBM to:

- Enhance trust and transparency by proactively addressing security concerns
- Ensure regulatory compliance requirements are met
- Define security best practices for use cases and business outcomes that are most important to you

Expected Outcomes

- Executive briefing on the security assessment of your Gen AI environment & applications
- Assessment of the maturity level of your security controls.
- Roadmap of implementation of security controls, key deliverables, and timelines
- Reference security architecture
- IBM's recommendation on next steps

Key Deliverables

IBM will work with you in a 2–5-day workshop to:

- Assess security for the entire Gen AI application lifecycle including:
    - Governance
    - Prompt injection
    - Insecure output handing
    - Modelling denial of service
    - Training data poisoning
    - Protecting sensitive data
    - Excessive agency
    - LLM overreliance
    - Model theft

- Define and refine a comprehensive security assessment that meets your exact business needs and ensures your Gen AI deployment is secure, trustworthy, and aligned with best practices.
- Recommend security enhancements for front end and backend security controls.
- Review technology mapping and reference architecture
- Prioritize security enhancements and agree on roadmap
- Present a proposed solution, high-level implementation plan, and costing

How to get started ↷

For more information or to schedule this workshop, speak with your sales representative or email sel@us.ibm.com