AI Security Frameworks

	Secure Software Development	Information Security and Cybersecurity	Risk Management	Safety and Trustworthiness
AI-specific	• Guidelines for secure AI system development (NCSC) ↪ • Machine learning principles (NCSC) ↪ • Security Testing of AI (SAI ETSI) ↪	• The Framework for AI Cybersecurity Practices (ENISA) ↪ • Mitigation Strategy Report (SAI ETSI) ↪ • AI Cyber Security Code of Practice (DSIT UK) ↪ • AI security concerns in a nutshell (BSI) ↪ • AI Security Risk Assessment (Microsoft) ↪ • Generative AI Security Scoping Matrix (Amazon) ↪	• ISO/IEC 23894: Guidance on risk management ↪ • Artificial Intelligence Risk Management Framework (NIST) ↪ • AI Model Risk Management Framework (CSA) ↪	• ISO/IEC 5469: Functional Safety and AI Systems ↪ • ISO/IEC 24028: Overview of trustworthiness in artificial intelligence ↪ • Trustworthy Artificial Intelligence (IEEE) ↪ • ANSI/CTA 2096: Guidelines for Developing Trustworthy Artificial Intelligence Systems ↪
AI-enabled	• Secure-by-Design (CISA) ↪ • Secure Software Development Framework (NIST) ↪	• ISO/IEC 27001: Information security, cybersecurity and privacy protection ↪ • Cybersecurity Framework (NIST) ↪	• ISO/IEC 31000: Risk management ↪	• EU's product safety legislation ↪

https://github.com/Xci-Gen/ai_security