SCENARIO

You have been assigned to perform an internal security audit for a fictional company:

ToySecure Inc. is a mid-sized U.S.-based business specializing in designing and selling children's toys. They operate from a single physical location that functions as their headquarters, retail store, and storage facility for inventory. Over time, their e-commerce platform has grown significantly, attracting buyers across the U.S. and internationally. Because of this rapid online expansion, the company's IT team is facing increased demands to maintain systems that support global operations.

The head of the IT department has determined that a thorough internal IT audit is necessary. She is concerned about sustaining compliance with industry standards and ensuring operational continuity as the business scales without a formalized strategy. She believes this audit will strengthen the company's security posture and help identify weaknesses, vulnerabilities, or risks to critical assets. Additionally, she wants to confirm that the organization meets legal and regulatory requirements for processing online payments and conducting business within the European Union (E.U.).

To address these concerns, the IT manager has adopted the NIST Cybersecurity Framework (NIST CSF) as the foundation for the audit. She has already set the scope and objectives for the audit, compiled an asset inventory managed by the IT team, and performed an initial risk assessment. The primary goal of the audit is to provide an overview of potential security gaps and the risks or penalties the company could face if issues remain unresolved.

My role: Review the IT manager's defined scope, objectives, and risk assessment report. Then, complete an internal audit by filling out a controls and compliance checklist based on the provided framework.