ToySecure Inc.: Audit Scope, Goals, and Risk Assessment Report

---

Scope and Goals of the Audit

Scope:
The audit will cover the full security framework implemented at ToySecure Inc. This includes all digital and physical assets managed by the IT department, such as employee devices, internal networks, and enterprise systems. The review will also examine existing security controls and compliance measures currently in place.

Goals:
The main objective is to evaluate the company's current assets and security posture, identify gaps, and complete a **controls and compliance checklist**. The ultimate goal is to recommend best practices and improvements to strengthen ToySecure Inc.'s security strategy.

Current Assets Managed by IT

- **On-premises infrastructure** supporting day-to-day business operations
- **Employee devices:** desktops, laptops, smartphones, remote workstations, peripherals (headsets, keyboards, mice, docking stations), and surveillance cameras
- **Retail and inventory assets:** products stored in the warehouse and available both in-store and online
- **Core business systems and services:** accounting software, telecom systems, database servers, security tools, e-commerce platform, and inventory management solutions
- **Internet connectivity and internal network infrastructure**
- **Data retention systems and storage solutions**
- **Legacy systems:** outdated systems still in use that require manual monitoring and maintenance

---

Risk Assessment

Risk Description:
Currently, asset management is inadequate, and several critical controls are missing. There are concerns about compliance with U.S. regulations and international standards, particularly those related to payment processing and customer data protection.

Control Best Practices Needed:

The **first function of the NIST Cybersecurity Framework (Identify)** highlights the importance of knowing and classifying all assets. ToySecure Inc. must invest resources in identifying its assets, categorizing them based on importance, and assessing the business impact if these assets were compromised or lost.

Risk Score:

8/10 (High) – This score reflects the lack of comprehensive controls and insufficient compliance measures.

Additional Observations

- All employees currently have broad access to internal data, which may include **cardholder data and sensitive customer information (PII/SPII)**.
- **Credit card data is not encrypted**, posing a serious confidentiality risk.
- **Least privilege access control** and **segregation of duties** are not enforced.
- The IT department maintains **data availability and integrity** but lacks other critical controls.
- **Firewall protection** is in place with well-defined rules, and **antivirus software** is installed and actively monitored.
- There is **no Intrusion Detection System (IDS)** deployed.
- **Disaster recovery plans and data backups** are nonexistent, leaving the company vulnerable to catastrophic data loss.

- The IT team has a procedure to **notify E.U. customers within 72 hours** of a breach and enforces privacy policies internally.

- **Password policy** exists but does not meet modern complexity standards (e.g., minimum eight characters, mix of letters, numbers, and symbols).

- No **centralized password management system** exists, which leads to inefficiencies in password reset and recovery.

- **Legacy systems** are maintained but lack a structured maintenance schedule or response plan.

- Physical security measures (locks, CCTV, fire detection) at the company's main office, store, and warehouse are up-to-date and functioning properly.