# Botium Toys - Full Audit Checklist (Controls + Compliance + Reasons)

## Controls Assessment

**Least Privilege** — **NO**
Reason: Employees have access to all internal data including PII and cardholder data; no restriction in place.

**Disaster Recovery Plans** — **NO**
Reason: Botium Toys currently has no disaster recovery or business continuity plans.

**Password Policies** — **YES**
Reason: A password policy exists, but it is weak and needs to be strengthened.

**Separation of Duties** — **NO**
Reason: Roles are not separated, creating potential conflict and increasing risk.

**Firewall** — **YES**
Reason: The IT department maintains a firewall with active rules.

**Intrusion Detection System (IDS)** — **NO**
Reason: Botium Toys does not have any IDS in place.

**Backups** — **NO**
Reason: No backup system or data recovery strategy exists.

**Antivirus Software** — **YES**
Reason: Antivirus is installed and regularly monitored.

**Legacy System Monitoring** — **YES**
Reason: Legacy systems are monitored, though the monitoring lacks a schedule.

**Encryption** — **NO**
Reason: Cardholder and sensitive data are stored unencrypted.

**Password Management System** — **NO**
Reason: There is no centralized password management system.

**Physical Locks** — **YES**
Reason: Physical access controls such as locks are in place.

**CCTV Surveillance — YES**
Reason: CCTV systems are up to date and functional.

**Fire Detection & Prevention — YES**
Reason: Fire alarms and sprinklers are operational.

## Compliance Checklist

**PCI DSS — NO**
Reason: Cardholder data is not encrypted, and several required security controls are missing.

**GDPR — NO**
Reason: PII is not sufficiently protected and no formal GDPR-compliant processes exist.

**SOC 2 — NO**
Reason: Botium Toys lacks required internal controls, monitoring, and documentation for SOC compliance.