Controls Assessment Checklist

- Least Privilege: No (Access controls are not properly implemented)
- Disaster Recovery Plans: No (No disaster recovery plans currently in place)
- Password Policies: No (Existing policies do not meet complexity requirements)
- Separation of Duties: No (Not properly implemented)
- Firewall: Yes (Firewall is in place and operational)
- Intrusion Detection System (IDS): No (Not installed)
- Backups: No (Critical data backups are missing)
- Antivirus Software: Yes (Installed and monitored)
- Manual Monitoring, Maintenance, and Intervention for Legacy Systems: No (No regular schedule or clear intervention methods)
- Encryption: No (Customer credit card information is not encrypted)
- Password Management System: No (No centralized system enforcing policy)
- Locks (offices, storefront, warehouse): Yes (Sufficient physical security measures are in place)
- Closed-circuit Television (CCTV) Surveillance: Yes (Surveillance system is up-to-date)
- Fire Detection/Prevention: Yes (Adequate systems are in place)

Compliance Checklist

PCI DSS

- Only authorized users have access to customers' credit card information: No (All employees currently have access)
- Credit card information is securely processed and stored: No (Lack of encryption and secure environment)
- Implement data encryption procedures: No (Not currently encrypted)
- Adopt secure password management policies: No (Policies not in line with standards)

GDPR

- E.U. customers' data is kept private/secured: Yes (Privacy policies developed and enforced)
- Plan in place for breach notification within 72 hours: Yes (Plan established)
- Data properly classified and inventoried: No (Inadequate data management practices)

- Enforce privacy policies and processes: Yes (Policies and processes are enforced)

SOC (Type 1 and Type 2)

- User access policies established: No (Inadequate access controls)
- Sensitive data (PII/SPII) is confidential/private: No (Inadequate controls on data privacy)
- Data integrity ensures accuracy and validation: Yes (Controls in place for data integrity)
- Data available to authorized individuals: Yes (Managed but needs improvement)

Recommendations

To improve Botium Toys' security posture, the IT manager should prioritize implementing the following:

- Enhance access controls by establishing least privilege and separation of duties.
- Develop and implement disaster recovery and data backup plans.
- Upgrade password policies and establish a centralized password management system.
- Implement encryption for sensitive customer data, particularly for credit card information.
- Install an intrusion detection system (IDS) to monitor network traffic for suspicious activity.
- Regularly review and update compliance with PCI DSS, particularly in data encryption and access control.
- Enhance data classification and inventory processes to better comply with GDPR requirements.