Project Title: Cybersecurity Audit for Botium Toys

Prepared by: MOHANAD DALOL

Purpose: This document represents a simulated cybersecurity audit for Botium Toys, a fictional company, designed for academic and educational purposes. It comprehensively overviews cybersecurity controls, compliance, and risk assessments.

Table of content

1. Introduction

This report comprehensively evaluates the cybersecurity posture of Botium Toys, a fictional company. This audit aims to identify potential vulnerabilities, evaluate compliance with industry standards, and propose actionable recommendations to improve the organization's security framework.

The scope of this assessment includes examining key cybersecurity controls, compliance with regulations such as PCI DSS and GDPR, and identifying risks to critical assets and business continuity.

Disclaimer: This is a simulated exercise created for educational purposes as part of a cybersecurity training activity. The findings, recommendations, and scenarios presented in this report are hypothetical and do not reflect any real-world organization or data.

2. Scope

- **Systems Covered:** On-premises infrastructure, employee workstations, online payment processing systems, and customer data storage.
- **Exclusions:** Third-party vendor systems and physical security unrelated to IT operations.

3. Findings

Controls Checklist Results

Control	Status
Least Privilege	Not Implemented
Disaster Recovery Plans	Not Implemented
Password Policies	Weak
Intrusion Detection System (IDS)	Not Implemented

Compliance Results

Regulation	Status
PCI DSS	Not Compliant
GDPR	Not Compliant

4. Risk Assessment

Summary

This risk assessment identifies key vulnerabilities in Botium Toys' IT systems, emphasizing areas requiring immediate attention to avoid regulatory fines and operational disruptions.

Overall Risk Score: 8/10 (High Risk).

Findings

- **Key Issues:**
    1. Lack of encryption for sensitive data.
    2. No Intrusion Detection System (IDS) for monitoring.
    3. Inadequate disaster recovery planning.
    4. Weak password management policies.
- **Impacts:**
    1. Increased risk of data breaches.
    2. Non-compliance with GDPR and PCI DSS regulations.
    3. Potential financial penalties and loss of customer trust.

5. Recommendations

High Priority:

1. Implement encryption for sensitive customer and business data.
2. Establish a robust backup and disaster recovery system.
3. Deploy an Intrusion Detection System (IDS) to monitor network activity.

Medium Priority:

1. Enforce least privilege to minimize unnecessary data access.
2. Improve asset classification and regularly update inventories.

6. **Detailed Checklists**

Controls Checklist

Control	**Status**
Least Privilege	No
Password Policies	Weak
Firewall	Yes
Antivirus Software	Yes
Intrusion Detection System (IDS)	No

Compliance Checklist

Regulation	**Best Practice**	**Status**
PCI DSS	Encryption of cardholder data	No
GDPR	Data classification and inventory	No
SOC	User access policies	No