Security Controls Assessment

Prepared by: Ammar Ibrahim
Course: Google Cybersecurity Certificate
Date: 25/2025

Introduction

Below is the internal IT security audit report for Botium Toys. The intent of this assessment is to compare the organization's current security position to the NIST Cybersecurity Framework. The audit summarizes in-place controls, suggests compliance with best practices, and assesses potential risks to business continuity, regulatory compliance, and protecting critical assets. Recommendations and findings provided in this report can be used by Botium Toys to improve its overall security position.

Scope and Objectives

Scope:

The internal audit will cover Botium Toys' IT system, physical facilities at their headquarters, storefront, and warehouse, and online systems that support the company's growing e-commerce operations. The audit will focus on detecting vulnerabilities, risks, and compliance shortfalls in the following:

- Information security controls (technical, administrative, and physical)
- Data handling and storage procedures, including payment and personal customer information
- Compliance with industry standards like PCI DSS, GDPR, and SOC requirements
- Disaster recovery, business continuity, and backup procedures
- Objectives:

The audit will:

- Discover inherent security vulnerabilities and threats to valuable assets.
- Ensure that IT infrastructure is compliant with regulatory requirements and industry best practice.
- Provide actionable suggestions to improve security posture and provide business continuity.
- Enable Botium Toys' growth while ensuring compliant and secure operations, especially for international customers.

Control / Best Practice	Yes / No	Recommendation
Minimizes attack surface	Yes	Regularly scan ports and services to remove unnecessary features.
Principle of least privilege	No	Restrict user privileges to the minimum required for tasks.
Defense in depth	Yes	Maintain multiple layers: firewall, antivirus, secure configs.
Separation of duties	No	Require multiple authorized staff input for critical tasks.
Keep security simple	Yes	Reduce unnecessary complexity in workflows and configs
Fix security issues correctly	No	Implement proper patch management and verify fixes.
Establish secure defaults	Yes	Ensure default settings are secure for new systems and users.
Fail securely	Yes	Configure systems to return to their most secure configuration in case of failure.
Don’t trust services	No	Enforce third-party vendors to follow security best practices.
Avoid security by obscurity	Yes	Security should rely on robust controls, not secrecy.

Summary and Recommendations:

The audit finds numerous good controls that are in place, such as up to date software and regulatory compliance. Areas for improvement include network access restrictions and full encryption of sensitive data. The performing of these recommendations will strengthen security posture and reduce potential risks.