Preview

**This audit doc is a first training exercise realized through the google certification. The goal of this exercise is assure i have known all the basic concepts of a security audit. ensure that security checks are made, to monitor for threats, risks, or vulnerabilities that can affect an organization’s business continuity and critical assets.**

*his scenario is based on a fictional company:*

Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and warehouse for their products. However, Botium Toy’s online presence has grown, attracting customers in the U.S. and abroad. As a result, their information technology (IT) department is under increasing pressure to support their online market worldwide.

The manager of the IT department has decided that an internal IT audit needs to be conducted. She's worried about maintaining compliance and business operations as the company grows without a clear plan. She believes an internal audit can help better secure the company’s infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to internally processing and accepting online payments and conducting business in the European Union (E.U.).

The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.

Your task is to review the IT manager’s scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Audit scope and goals

**Summary:** The scope of this audit was defined as the entire security program of Botium Toys, including assets, internal networks and systems. The goals are to ensure that the high growth of the online activities can continue safely, without bringing high risks to the company assets or affecting the business operation. For this purpose, the audit aimed to conform the company’s safety standard with the legislation.

**Scope:** The internal IT audit will assessed the following:

* Current Assets
* Risk Assessment
* Security Controls

**Goals:** Assess current security controls and check which controls and compliance pratices needed to be implemented

* Implementation of security controls
* Law compliance

**Risk assessment**

**Current assets** of Botium Toys include:

* On-premises equipment for in-office business needs
* Employee equipment: end-user devices (desktops/laptops, smartphones),
* remote workstations, headsets, cables, keyboards, mice, docking stations,
* surveillance cameras, etc.
* Storefront products available for retail sale on site and online; stored in the
* company’s adjoining warehouse
* Management of systems, software, and services: accounting,
* telecommunication, database, security, ecommerce, and inventory management
* Internet access
* Internal network
* Data retention and storage
* Legacy system maintenance: end-of-life systems that require human monitoring

**Risk description**

Proper security controls and law compliance aren’t in place. This may lead to **sensitivy data breach, identification thef, government fines and permanent data loss**.

**Risk score**

In a scale of 1 to 10, the risk score is 9. Due to the lack of security controls and law compliance, the bussiness continuity is at stake, with huge reputation, financial and assets loss.

Controls and compliance assessment checklist

| **Administrative Controls** | | | |
| --- | --- | --- | --- |
| **Control name** | **Control type and explanation** | **Needs to be implemented**  **(X)**  **Already implemented ( )** | **Priority** |
| Password policies | Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques | X | High |
| Manual Monitoring for legacy systems | Preventive; Refers to the process of actively overseeing old systems | X | Medium |
| Disaster Recovery Plan | Corrective; A strategy that outlines how recover from a disruptive event | X | High |
| Least Privilage | Preventive; A policy-driven practice that ensures only the needed access will be granted to authorized people. | X | High |
| Separation of Duties | Preventive; Distributes access in a way that avoids the centralization of power in one individual | X | Medium |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Technical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)**  **Already implemented ( )** | **Priority** |
| Intrusion Detection System (IDS) | Detective; allows IT team to identify possible intrusions (i.e., anomalous traffic) quickly | X | HIgh |
| Encryption | Deterrent; makes confidential information/data more secure (i.e., website payment transactions) | X | High |
| Network Firewall | Preventive; Protects a network from unauthorized acces by monitoring and controlling network traffic. |  |  |
| Antivírus Software | Preventive, Detective and Corrective; Software used to prevent, detect and eliminate malware and viruses. |  |  |
| Backup | Corrective control; Prevent permanent data loss by saving copies. | X | High |
| Password management system | Preventive; A tool that helps protect, acess and manage passwords | X | Medium |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Physical Controls** | | | |
| **Control Name** | **Control type and explanation** | **Needs to be implemented**  **(X)**  **Already implemented ( )** | **Priority** |
| Closed-circuit television (CCTV) surveillance | Preventative/detective; can reduce risk of certain events; can be used after event for investigation |  |  |
| Locks | Preventative; physical and digital assets are more secure |  |  |
| Fire Dectetion | Preventive; Provides early warnings of fire hazards that could disrupt or damage assets |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Compliance Checklist** | | | |
| **Compliance Name** | **Explanation** | **Needs to be implemented**  **(X)**  **Already implemented ( )** | **Priority** |
| Payment Card Industry Data Security Standards (PCI DSS) | A set of security standards designed to ensure the correct handling of credit card information and payment data | X | High |
| General Data Protection Regulation (GDPR) | Privacy and data regulation implemented by the European Union. | X | High |
| System and Organizations Controls (SOC Type1, SOC Type 2) | Developed by American Institute of Certified Public Accountants, they are used to evaluate internal controls and pratices of organizations providing services to third parties. | X | High |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

RECOMMENDATIONS

This company currently has the following threads and vulnerabilities.

**Threat actors**

This company is exposed to multiple threat actors, internal and external.

* **Employers**: Since all employers have data access, this may lead to a data leak, whether intentionally or not;
* **Hackers:** The company has several vulnerabilities that may lead to an attack. For example, the company does not have a strong password policy and is vulnerable to a brute force attack.

**Vulnerabilities**

1. **Software Vulnerabilities**: This company does not have a security control for manual monitoring, maintenance and intervention for legacy systems. This may lead to outdated security patches;
2. **Inside threats**: Since all employers have data access, this may lead to an intentionally or unintentionally breach through negligence or malicious actions;
3. **Brute Force Attack**: The lack of a good password policy may lead to a succeful brute force attack or dictionary attack;
4. **Permanent data loss:** No backup means a disruptive event can lead to permanent data loss;
5. **Excessive privileges:** The overconcentration of access and duties can lead to misuse of data or information;
6. **Bussiness continuity:** The lack of a recovery plans will lead to operation gasp and financial impact
7. **Low guard:** This company runs without a Intrusion Detection System (IDS), causing a detection failure, responde and prevetion;
8. **Legal and reputation vulnerability:** Non-compliance with the law or international standards can lead to financial health loss and reputation loss.

To ensure a robust cybersecurity posture, mitigate risk, and meet legal and regulatory requirements, the company should adopt all the security measures outlined in the checklist. It must also adopt the regulatory and legal standards of (PCI DSS), (GDPR) and (SOC Type1, SOC Type2).