Audit Report 10-05-2024 #1

Glow Clothing - San Lorenzo 3175 Eldorado Misiones

# Risk assessment, objectives and scope

## Audit Scope:

The scope of this audit is defined as Botium Toys' entire security program. This includes its assets, such as employee equipment and devices, its internal network, and its systems. You will need to review the assets Glow Clothing has and the compliance controls and practices they have in place.

## Audit objectives:

Existing assets will be assessed and the compliance and controls checklist will be completed to determine what compliance controls and best practices need to be implemented to improve Glow Clothing’s security posture.

## Current assets

Assets managed by the IT Department include:

* Local equipment for business needs in the office
* Employee Equipment: End-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
* Showcase products available for retail sale on-site and online; stocked in the company's adjacent warehouse
* Systems, software and services management: accounting, telecommunications, databases, security, e-commerce and inventory management.
* Internet access
* Internal network
* Data retention and storage
* Legacy Systems Maintenance – End-of-Life Systems Requiring Human Monitoring

## risk assessment

Currently, there is inadequate asset management. In addition, Glow Clothing does not have all the appropriate controls in place and may not be in full compliance with US and international regulations and standards.

## Monitoring best practices

The first of the five NIST CSF functions is Identify. Glow Clothing will need to dedicate resources to identifying assets so they can be properly managed. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity .

### Risk score

On a scale of 1 to 10, the risk score is 8, which is quite high. This is due to a lack of controls and adherence to compliance best practices.

### Additional comments

The potential impact of an asset loss is rated as medium because IT does not know which assets would be at risk. The risk to assets or fines from governing bodies is high because Glow Clothing does not have all necessary controls in place and is not in full compliance with best practices related to compliance with regulations that keep critical data private and secure. Please review the following bullet points for specific details:

* Currently, all Glow Clothing employees have access to internally stored data and may access cardholder data and customer PII/SPII.
* Currently, encryption is not used to ensure the confidentiality of customer credit card information that is accepted, processed, transmitted and stored locally in the company's internal database.
* Access controls related to least privilege and separation of duties have not been implemented.
* The IT department has ensured availability and built in controls to ensure data integrity.
* The IT department has a firewall that blocks traffic based on a set of appropriately defined security rules.
* The IT department installs and regularly monitors anti-virus software.
* The IT department has not installed an intrusion detection system (IDS).
* There are currently no disaster recovery plans and the company has no backups of critical data.
* The IT department has established a plan to notify EU customers within 72 hours if there is a security breach. In addition, privacy policies, procedures, and processes have been developed and enforced between members of the IT department and other employees to properly document and maintain data.
* Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
* There is no centralized password management system to enforce minimum password policy requirements, which sometimes impacts productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
* While legacy systems are monitored and maintained, there is no regular schedule for these tasks and intervention methods are unclear.
* The physical location of the store, which includes Glow Clothing's main offices, store front, and product warehouse, has sufficient locks, up-to-date closed circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.