Audit Scope and Goals

Summary: The internal audit needs to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as “high risk,” and present an overall strategy to improve the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

Scope: The internal IT audit will assess the following:

- Assess user permissions
- Identify existing controls, procedures, and system protocols
- Account for technology currently in use

Goals: The goals for the internal IT audit are:

- Adhere to the NIST Cybersecurity Framework (CSF)
- Establish policies and procedures to ensure compliance with regulations
- Fortify system controls

Risk Assessment

Current assets

Assets managed by the IT Department include:

- Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Internal network: protected storage of customer, vendor, organizational data

Risk description

Currently, there is inadequate management of assets. Additionally, proper controls are not in place and the organization may not be compliant with U.S. and international compliance regulations and standards.

Control best practices

The organization will need to dedicate resources to managing assets. Additionally, they will need to determine the impact of the loss of existing assets, including systems, on business continuity.

Risk score

On a scale of 1-10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to necessary compliance regulations and standards.

Additional comments

The likelihood of a lost asset or fines from governing bodies is high because the organization does not have all of the necessary controls in place and is not adhering to required regulations and standards related to keeping PII data private.

Controls Assessment

Administrative Controls			
Control name	**Control type and explanation**	**Needs to be implemented (X)**	**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

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**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/ Medium

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for	X	High/ Medium

	investigation		
Locks	Preventative; physical and digital assets are more secure	X	High

Compliance Checklist

☑ **General Data Protection Regulation (GDPR)**

GDPR is a European Union (EU) general data regulation that protects the processing of EU citizens' data and their right to privacy in and out of EU territory. Additionally, if a breach occurs and a EU citizen's data is compromised, they must be informed within 72 hours of the incident.

Explanation: The organization needs to adhere to GDPR because we conduct business and collect personal information from people in the EU.

☑ **Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Explanation: The organization needs to adhere to PCI DSS because we store, accept, process, and transmit credit card information in person and online.