Performing an Internal Audit

IT security professionals help minimize risks to organizations and people.

In this project I will conduct an internal security audit for a fictional company:

EffVarTech is a US tech startup founded in 2015. The company has one physical location, however its online presence has grown attracting customers around the world. The company IT department is under increasing pressure to support company's online market worldwide. The IT manager has decided that an internal IT audit would need to be conducted. She expresses concerns about not having a solidified plan of action to ensure business continuity and compliance, as the business grows. 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 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, and completing a risk assessment. The goal of the audit is to provide an overview of the risks the company might experience due to the current state of their security posture. The IT manager wants to use the audit findings as evidence to obtain approval to expand his department.

Instructions: Review the guidelines in the email from the IT manager along with the manager's Scope and goals, and Risk assessment documents, then perform an internal audit to complete a controls assessment and compliance checklist. Below is a copy of the IT Manager's email:

Hello,

I have completed the EffVarTech ' Audit scope and goals, as well as a Risk assessment. At a high level, the main goals and risks are as follows:

<u>Goals:</u>

-Improve company's security posture, by aligning to industry best practices (e.g., adhere to the NIST CSF, implement concept of least permissions)

-Provide mitigation recommendations (i.e., controls, policies, documentation) based on current risks

-Identify compliance regulations EffVarTech must adhere to, primarily based on where we conduct business and how we accept payments.

Please review the full report in the "EffVarTech Audit scope and goals" document attached.

<u>Risks:</u>

-Inadequate management of assets

-Proper controls are not in place

-May not be compliant with US and international regulations and guidelines

-Current risk score is 8/10 (high), due to a lack of controls and adherence to compliance regulations and standards.

Please review the complete list of assets and risks in the "EffVarTech Risk assessment" document to this email.

Thank you,
EffVarTech IT Manager

Below is a copy of:

EffVaTech Audit scope and goals

Summary: Perform an audit of EffVaTech' cybersecurity program. The 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 for improving the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

Scope:

[Note that the scope is not constant from audit to audit. However, once the scope of the audit is clearly defined, only items within scope should be audited. In this scenario, the scope is defined as the entire security program. This means all assets need to be assessed alongside internal processes and procedures.]

EffVaTech internal IT audit will assess the following:

- Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
- Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
- Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
- Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
- Ensure current technology is accounted for. Both hardware and system access.

Goals:

[*Note that the goal of an audit is the desired deliverables or outcomes]*

The goals for EffVaTech' internal IT audit are:

- To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for their systems to ensure they are compliant
- Fortify system controls
- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

Below is a copy of:

EffVaTech Risk assessment

Current assets

Assets managed by the IT Department 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.
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
- Internet access
- Internal network
- Vendor access management
- Data center hosting services
- Data retention and storage
- Badge readers
- Legacy system maintenance: end-of-life systems that require human monitoring

Risk description

Currently, there is inadequate management of assets. Additionally, EffVaTech does not have the proper controls in place and may not be compliant with US and international regulations and standards.

Control best practices

The first of the five functions of the NIST CSF is Identify. EffVaTech 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 to 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 potential impact from the loss of an asset is rated as medium, because the IT department does not know which assets would be lost. The likelihood of a lost asset or fines from governing bodies is high because EffVaTech does not have all of the necessary controls in place and is not adhering to required regulations and standards related to keeping customer data private.