Perform a security audit

**Activity Overview**



In part one of this activity, you will conduct an internal security audit, which you can include in your cybersecurity portfolio. To review the importance of building a professional portfolio and options for creating your portfolio, read [Create a cybersecurity portfolio](https://www.coursera.org/learn/manage-security-risks/resources/pyALD).

As a reminder, audits help ensure that security checks are made, to monitor for threats, risks, or vulnerabilities that can affect an organization’s business continuity and critical assets.

Be sure to complete this activity and answer the questions that follow before moving on. The next course item will provide you with a completed exemplar to compare to your own work.

**Scenario**



Review the following scenario. Then complete the step-by-step instructions.

*This 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 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 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.

**Step-By-Step Instructions**



Follow the instructions to complete each step of the activity. Then, answer the 5 questions at the end of the activity before going to the next course item to compare your work to the completed exemplar.

According to the scenario, several controls and compliance best practices are not currently in place. These areas represent potential areas of improvement that should be addressed to enhance Botium Toys' security posture and compliance with regulations.