Portfolio Activity: Conduct a security audit

To pass this course item, you must complete the activity and receive at least 80%, or 4 out of 5 points, on the questions that follow. Once you have completed the activity and questions, review the feedback provided.

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.

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.

Create a cybersecurity portfolio:

Throughout this certificate program, you will have multiple opportunities to develop a professional cybersecurity portfolio to showcase your security skills and knowledge.
In this reading, you’ll learn what a portfolio is and why it’s important to develop a professional cybersecurity portfolio. You’ll also learn about options for creating an online or self-hosted portfolio that you can share with potential employers when you begin to look for cybersecurity jobs.

What is a portfolio, and why is it necessary?

Cybersecurity professionals use portfolios to demonstrate their security education, skills, and knowledge. Professionals typically use portfolios when they apply for jobs to show potential employers that they are passionate about their work and can do the job they are applying for. Portfolios are more in depth than a resume, which is typically a one-to-two page summary of relevant education, work experience, and accomplishments. You will have the opportunity to develop a resume, and finalize your portfolio, in the last course of this program.

Options for creating your portfolio:

There are many ways to present a portfolio, including self-hosted and online options such as:

- Documents folder
- Google Drive or Dropbox
- Google Sites
- Git repository

Option 1: Documents folder

Description: A documents folder is a folder created and saved to your computer's hard drive. You manage the folder, subfolders, documents, and images within it.
Document folders allow you to have direct access to your documentation. Ensuring that your professional documents, images, and other information are well organized can save you a lot of time when you're ready to apply for jobs. For example, you may want to create a main folder titled something like "Professional documents." Then, within your main folder, you could create subfolders with titles such as:

- Resume
- Education
- Portfolio documents
- Cybersecurity tools
- Programming

Setup: Document folders can be created in multiple ways, depending on the type of computer you are using. If you're unsure about how to create a folder on your device, you can search the internet for instructional videos or documents related to the type of computer you use.

Option 2: Google Drive or Dropbox

Description: Google Drive and Dropbox offer similar features that allow you to store your professional documentation on a cloud platform. Both options also have file-sharing features, so you can easily share your portfolio documents with potential employers. Any additions or changes you make to a document within that folder will be updated automatically for anyone with access to your portfolio.

Similar to a documents folder, keeping your Google Drive or Dropbox-based portfolio well organized will be helpful as you begin or progress through your career.

Setup: To learn how to upload and share files on these applications, visit the Google Drive and Dropbox websites for more information.

Option 3: Google Sites

Description: Google Sites and similar website hosting options have a variety of easy-to-use features to help you present your portfolio items, including customizable layouts, responsive webpages, embedded content capabilities, and web publishing. Responsive webpages automatically adjust their content to fit a variety of devices and screen sizes. This is helpful because potential employers can review your content using any device and your media will display just as you intend. When you’re ready, you can publish your website and receive a unique URL. You can add this link to your resume so hiring managers can easily access your work.

Setup: To learn how to create a website in Google Sites, visit the Google Sites website.

Option 4: Git repository

Description: A Git repository is a folder within a project. In this instance, the project is your portfolio, and you can use your repository to store the documents, labs, and screenshots you complete during each course of the certificate program. There are several Git repository sites you can use, including:

- GitLab
- Bitbucket
- GitHub

Each Git repository allows you to showcase your skills and knowledge in a customizable space. To create an online project portfolio on any of the repositories listed, you need to use a version of Markdown.

Setup: To learn about how to create a GitHub account and use Markdown, follow the steps outlined in the document Get started with GitHub.

Portfolio projects

As previously mentioned, you will have multiple opportunities throughout the certificate program to develop items to include in your portfolio. These opportunities include:

- Drafting a professional statement
- Conducting a security audit
- Analyzing network structure and security
- Using Linux commands to manage file permissions
- Applying filters to SQL queries
- Identifying vulnerabilities for a small business
- Documenting incidents with an incident handler’s journal
- Importing and parsing a text file in a security-related scenario
- Creating or revising a resume

Note: Do not include any private, copyrighted, or proprietary documents in your portfolio. Also, if you use one of the sites described in this reading, keep your site set to “private” until it is finalized.

Key takeaways

Now that you’re aware of some options for creating and hosting a professional portfolio, you can consider these as you develop items for your portfolio throughout the certificate program. The more proactive you are about creating a polished portfolio, the higher your chances of impressing a potential employer and obtaining a new job opportunity in the cybersecurity profession.

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.

Step 1: Access supporting materials

The following supporting materials will help you complete this activity. Keep materials open as you proceed to the next steps.

To use the supporting materials for this course item, read Botium Toys Scope, goals, and risk assessment report.

Botium Toys: Scope, goals, and risk assessment report

Scope and goals of the audit

Scope: The scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.

Goals: Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys' security posture.

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.
- 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 assessment

Risk Description:

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be fully compliant with U.S. and international regulations and standards.

Control Best Practices:

The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to identify assets so they can appropriately manage them. 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 fairly high. This is due to a lack of controls and adherence to compliance best practices.

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 at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

- Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.

- Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.

- Access controls pertaining to least privilege and separation of duties have not been implemented.

- The IT department has ensured availability and integrated controls to ensure data integrity.

- The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.

- Antivirus software is installed and monitored regularly by the IT department.

- The IT department has not installed an intrusion detection system (IDS).

- There are no disaster recovery plans currently in place, and the company does not have backups of critical data.

- The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/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 that enforces the password policy's minimum requirements, which sometimes affects 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 in place for these tasks and intervention methods are unclear.

- The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

Controls and Compliance Checklist

To complete the controls assessment checklist, refer to the information provided in the
scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the **control categories** document.

Then, select “**yes**” or “**no**” to answer the question: Does Botium Toys currently have this control in place?

Controls Assessment

A controls assessment involves closely reviewing an organization’s existing assets and evaluating potential risks to those assets to ensure effective internal controls and processes.

Yes	No		Administrative/Managerial Controls
□	☑		Least Privilege
□	☑		Disaster Recovery Plans
□	☑		Password Policies
□	☑		Access Control Policies
□	☑		Account Management Policies
□	☑		Separation of duties

Yes	No		Technical Controls
☑	□		Firewall
□	☑		IDS/IPS
□	☑		Encryption
□	☑		Backups
□	☑		Password Management
☑	□		Antivirus (AV) Software

☑	□		Manual Monitoring, Maintenance, and Intervention Human Required Legacy systems

Yes	No		Physical/Operational Controls
□	☑		Time-Controlled Safe
□	☑		Adequate Lighting
☑	□		Closed-Circuit Television (CCTV)
☑	□		Locking Cabinets (for network gear)
□	☑		Signage Indicating Alarm Service Provider
☑	□		Locks - Warehouse, Storefront, and Offices of Products
☑	□		Fire Detection and Prevention (fire alarm, sprinkler system, etc.)

System and Organizations Controls (SOC type 1, SOC type 2)

The American Institute of Certified Public Accountants® (AICPA) auditing standards board developed this standard. The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels such as Associate, Supervisor, Manager, Executive, Vendor, and Others.

They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Yes	No		Best Practices, Organizations Follow Voluntarily, Manage Risk
□	☑		Sensitive Data (PII/SPII) is Confidential and Private
□	☑		Data is Available to Individuals Authorized to Access
☑	□		Data Integrity Ensures the Data is Consistent, Complete, Accurate, and has been Validated
□	☑		User Access Policies are Established

General Data Protection Regulation (GDPR)

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. residents' data and their right to privacy in and out of E.U. territory. For example, if an organization is not being transparent about the data they are holding about an E.U. citizen and why they are holding that data, this is an infringement that can result in a fine to the organization. Additionally, if a breach occurs and an E.U. citizen's data is compromised, they must be informed.

The affected organization has 72 hours to notify the E.U. citizen about the breach.

Yes	No		Best Practices, E.U. Citizen Privacy In and Out of E.U. Territories
□	☑		Verify that data is accurately classified and cataloged
☑	□		Privacy Protection Policies, Processes and Procedures are Documented and Maintain Data Integrity Properly
☑	□		72 Hours to notify the E.U. citizen about the breach
□	☑		E.U. Customer(s) Private Data Remains Secure

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. The objective of this compliance standard is to reduce credit card fraud.

Yes	No		Best Practices, Security Standard
□	☑		Adopt Audits for Enforcing Stricter Password and Management Policies
□	☑		Strict Policies for Authorized Users when Accessing Customer Credit Card
□	☑		Organization Storing Customer(s) Credit Card, Accepting, Processing and Transmitting it needs to be a Secured Environment
□	☑		Encrypting Confidential, and Private Data, Difficult to Decode for Unauthorized users

Center for Internet Security (CIS®)

CIS is a nonprofit with multiple areas of emphasis. It provides a set of controls that can be used to safeguard systems and networks against attacks. Its purpose is to help organizations establish a better plan of defense. CIS also provides actionable controls that security professionals may follow if a security incident occurs.

Control Categories

Administrative/Managerial Controls

Control Name	Control Type	Control Purpose	Requires Execution	Urgency
Least Privilege	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts. Principle of least privilege. Separation of duties: Critical actions should rely on multiple people, each of whom follows the principle of least privilege. Principle of least privilege: Users have the least amount of access required to perform their everyday tasks.	Yes	High
Disaster recovery plans	Corrective	Provide business continuity: An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans. Must have on-site and off-site backups and encrypted backups a minimum of three different kinds, one on-site with network and without network/connected to any internet/intranet and one or two that is connected to off-site security. UPS minimum of 24 hours, 3 days would be recommended if one can implement, and a week at best; how important is your business to stay up and	Yes	High

		running? Fire safety systems to protect against damage as much as possible.		
Password policies	Preventative	Reduce the likelihood of account compromise through brute force or dictionary attack techniques. Defense in depth. NIST Password Guidelines. Use a Password Manager for Increased Password Strength. Store Secrets Securely Through Salting and Hashing. Lock After Multiple Attempts. Employ Two-Factor Authentication or Multi-Factor Authentication.	Yes	Highest
Access control policies	Preventative	Bolster confidentiality and integrity by defining which groups can access or modify data. CIA. Protection, like encryption, safeguards data from being tampered with. Accessible to those who are authorized to access the data.	Yes	Medium
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting the overall impact from disgruntled former employees and default account usage. Minimize attack surface area. Security assessment and testing, security operations, and software development security. IAM.	Yes	Medium
Separation of duties	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts. Separation of duties: Critical actions should rely on multiple people, each of whom follows the principle of least privilege. Prevent individuals from carrying out fraudulent or illegal activities.	Yes	Medium

Technical Controls

Control Name	Control Type	Control Purpose	Requires Execution	Urgency
Firewall	Preventative	To filter unwanted or malicious traffic from entering the network	No	Medium
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule	Yes	Medium
Encryption	Deterrent	Provide confidentiality to sensitive information	Yes	Medium
Backups	Corrective	Restore/recover from an event	Yes	High
Password management	Preventative	Reduce password fatigue	Yes	Low
Antivirus (AV) software	Corrective	Detect and quarantine known threats	No	Low
Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems	Yes	High

Physical/Operational Controls

Control Name	Control Type	Control Purpose	Requires Execution	Urgency
Time-controlled safe	Deterrent	Reduce attack surface and overall impact from physical threats	Yes	Low
Adequate lighting	Deterrent	Deter threats by limiting “hiding” places	Yes	Low
Closed-circuit television (CCTV)	Preventative/ Detective	Closed circuit television is both a preventative and detective control because it’s presence can reduce risk of certain types of events from occurring, and can be used after an event to	No	Low

		inform on event conditions		
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear	No	Low
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful attack seem low	Yes	Low
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets	No	Low
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative	Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.	No	Low

Recommendations for IT Manager

Asset Management Improvement:

Implement a comprehensive asset management system to accurately inventory and track all IT assets, including hardware, software, and data.
Classify assets based on their criticality and importance to business operations to prioritize security measures accordingly.
Conduct regular audits to ensure that all assets are accounted for and properly managed.

Compliance Enhancement:

Ensure compliance with relevant regulations and standards, including those related to online payment processing and conducting business in the European Union.
Review and update privacy policies, procedures, and processes to align with regulatory requirements, especially concerning the protection of customer data.

Security Controls Strengthening:

Implement access controls, including the principle of least privilege and separation of duties, to restrict unauthorized access to sensitive data and systems.
Enhance encryption mechanisms to safeguard the confidentiality of customer credit card information and personally identifiable information (PII).
Deploy an intrusion detection system (IDS) to monitor network traffic and detect potential security breaches or unauthorized activities in real time.
Develop and test disaster recovery plans to ensure business continuity in the event of a security incident or data breach.

Password Management Enhancement:

Enforce stronger password policies that require a combination of alphanumeric characters, special symbols, and minimum length requirements.
Implement a centralized password management system to enforce password policies consistently across the organization and facilitate password recovery/reset processes.

Legacy System Maintenance and Monitoring:

Establish a regular maintenance schedule for legacy systems to ensure that they receive timely updates, patches, and security fixes.
Define clear intervention methods and protocols for addressing issues or vulnerabilities in legacy systems to mitigate risks effectively.

Physical Security Measures:

Review and update physical security measures, such as door locks, surveillance cameras, and fire detection systems, to maintain a secure physical environment for the company's premises and assets.
By addressing these areas of improvement, Botium Toys can enhance its security posture, mitigate risks, and ensure compliance with regulatory requirements, thereby safeguarding its critical assets and business operations.

Portfolio Activity Exemplar Conduct a Security Audit

The Controls and Compliance Checklist that I have created closely resembles the exemplar without the detailed explanation list. I recognize the importance of incorporating explanation(s) into my checklist assessment, as it would greatly enhance the evaluation process.

I have developed a complementary Control Categories document. This document includes two additional columns: 'Requires Execution' and 'Urgency.' These columns allow for a more thorough evaluation of control measures by indicating whether execution is needed and the level of urgency for implementation.

In the 'Requires Execution' column, controls are marked as either 'Yes' or 'No' to denote whether action is necessary. The 'Urgency' column categorizes controls as 'Highest,' 'High,' 'Medium,' or 'Low' based on their priority for implementation.

By integrating these additional elements, I aim to provide clearer insights into the evaluation process and facilitate informed decision-making regarding control implementation. Moving forward, I am committed to refining my assessment methods to ensure a comprehensive and effective approach to cybersecurity compliance."