Information Systems Risk Controls and Auditing Management

Practice Lab - Week 2

Introduction

**Introduction**

The Information Systems Risk Controls and Auditing Management module provides you with the instructions and devices to develop your hands on skills in the following topics.

* Reviewing Security Controls
* Selecting Security Controls
* Identifying Supporting Artifacts and Documentation

**Lab time:**It will take approximately 1 hour to complete this lab.

**Lab Diagram**

During your session you will have access to the following lab configuration. Depending on the exercises you may or may not use all of the devices, but they are shown here in the layout to get an overall understanding of the topology of the lab.



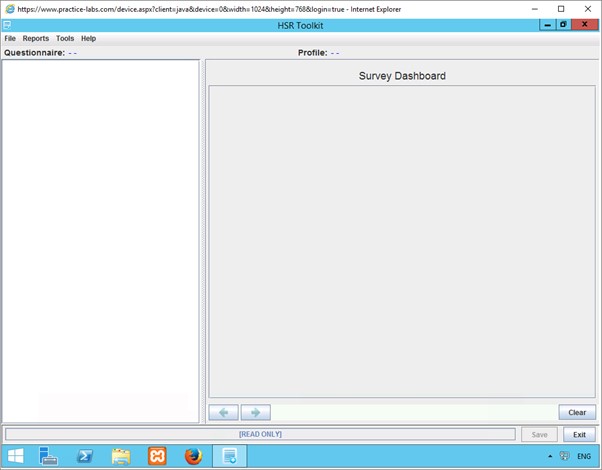
**Connecting to your lab**

In this module you will be working on the following equipment to carry out the steps defined in each exercise.

* **PLABWIN10**(Windows 10 Workstation)

You will be using the following software in this lab:

* **HSR Toolkit**



To start, simply choose a device and click **Power on**. In some cases, the devices may power on automatically.

For further information and technical support, please see our Help and Support page.   
This document and its content is copyright of Practice-IT - © Practice-IT 2015. All rights reserved. Any redistribution or reproduction of part or all of the contents in any form is prohibited other than the following:  
1. You may print or download to a local hard disk extracts for your personal and non-commercial use only.  
2. You may copy the content to individual third parties for their personal use, but only if you acknowledge the website as the source of the material. You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system.

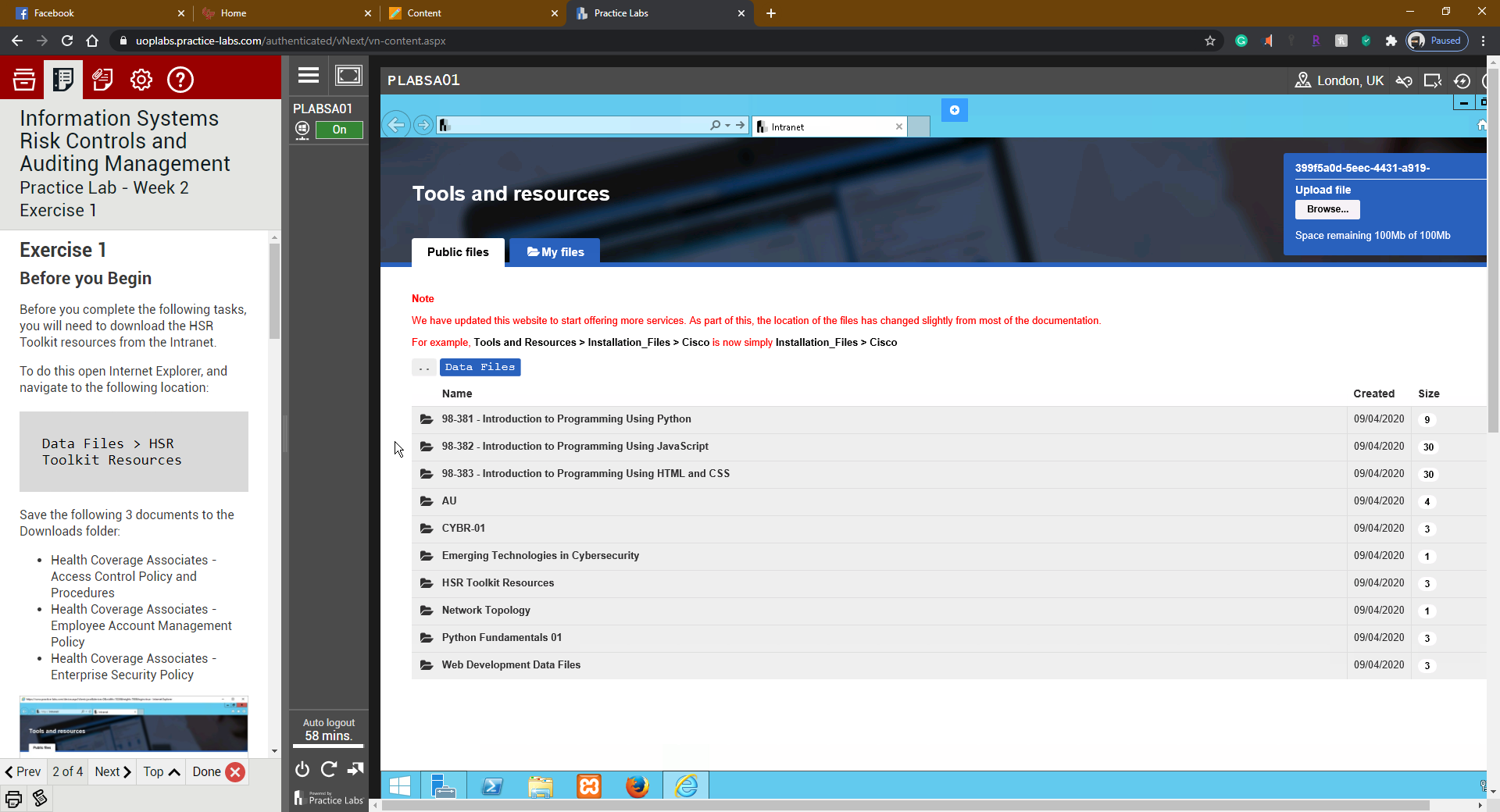
## Exercise 1

### Before you Begin

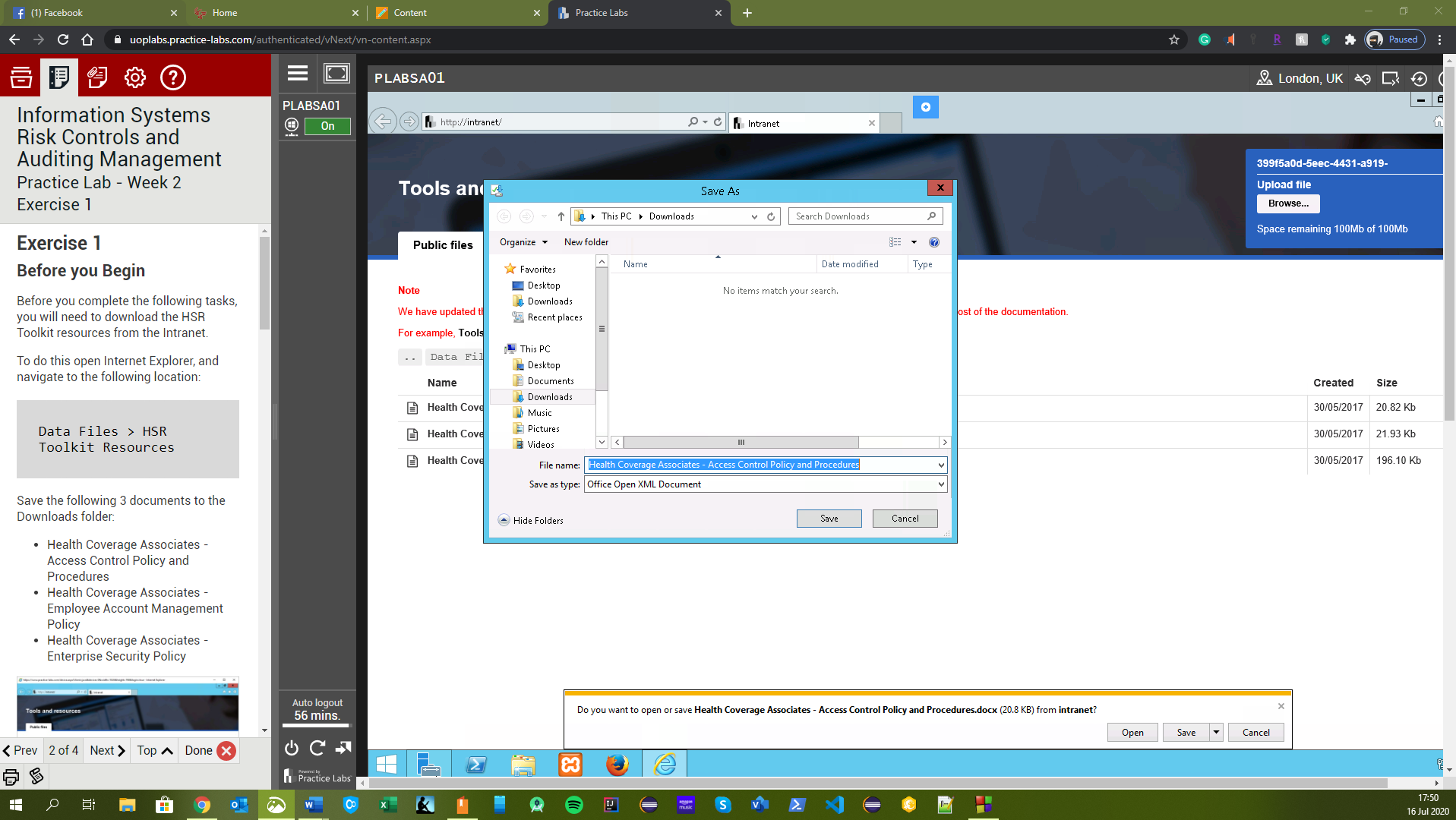
Before you complete the following tasks, you will need to download the HSR Toolkit resources from the Intranet.

To do this open Internet Explorer, and navigate to the following location:

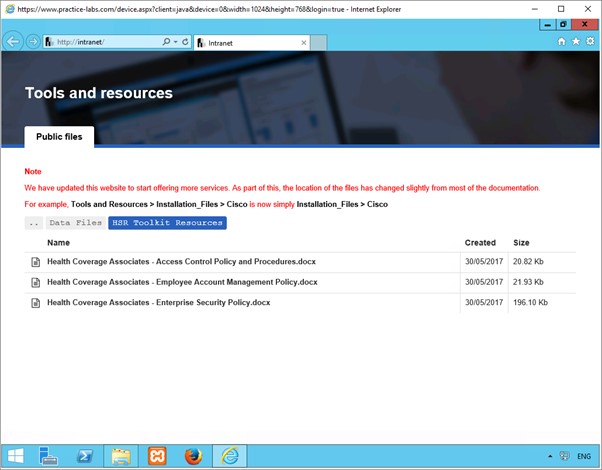
Data Files > HSR Toolkit Resources



Save the following 3 documents to the Downloads folder:



* Health Coverage Associates - Access Control Policy and Procedures
* Health Coverage Associates - Employee Account Management Policy
* Health Coverage Associates - Enterprise Security Policy



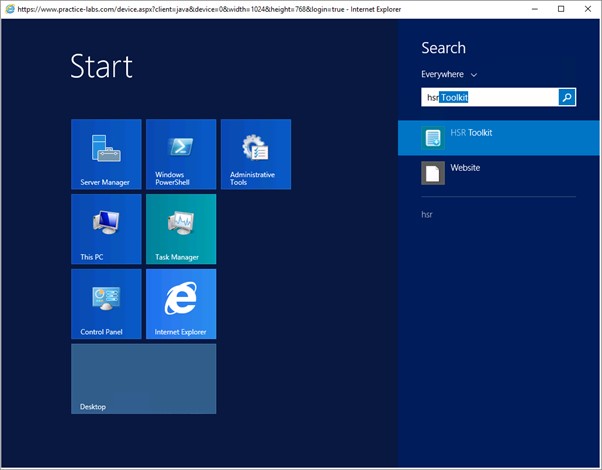
### Task 1: Open the NIST HSR Toolkit and Create a New Profile

#### Step 1

Click Start and type the following into the search bar:

hsr toolkit

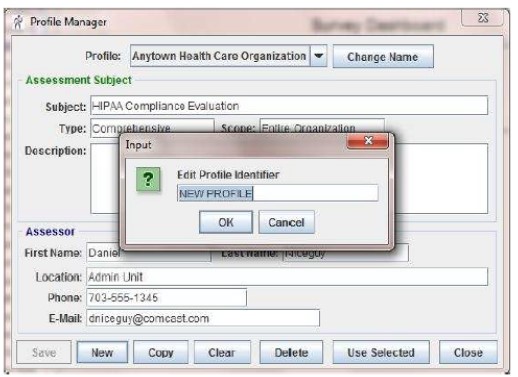
Click HSR Toolkit to launch the application.



#### 

#### Step 2

On the **Tools**tab, select **Profile Manager**. The Profile Manager window will appear.



#### Step 3

Select the **New**button. The Edit Profile Identifier box will appear.

#### Step 4

Fill in “**Health Coverage Associates**” and select OK.

#### Step 5

Fill in the rest of the profile information on the assessment subject and the assessor.

Subject: “Risk Assessment”

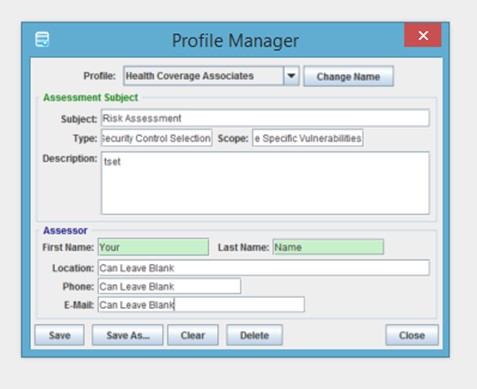
Type: “Security Control Selection”

Scope: “Three Specific Vulnerabilities”

Description: “Week 2 Lab”

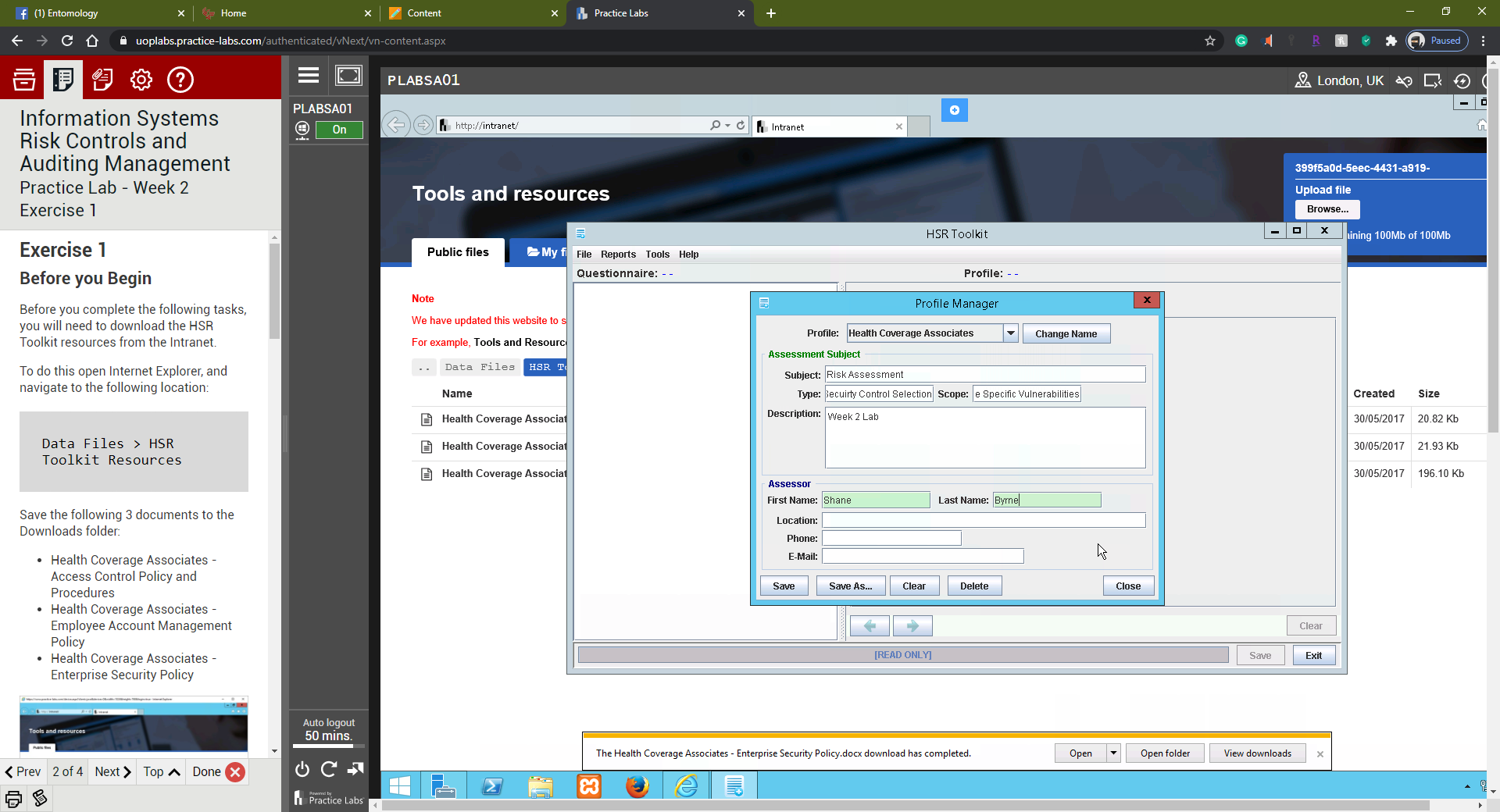
First Name: Your First Name

Last Name: Your Last Name



#### Step 6

Capture a screen shot



#### Step 7

Click **Save**

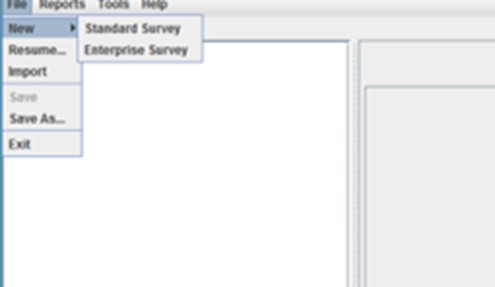
### Task 2: Open a New Survey

#### Step 1

On the **File**tab, select **New**to populate a new survey. The **Profile Manager**screen will appear.

#### Step 2

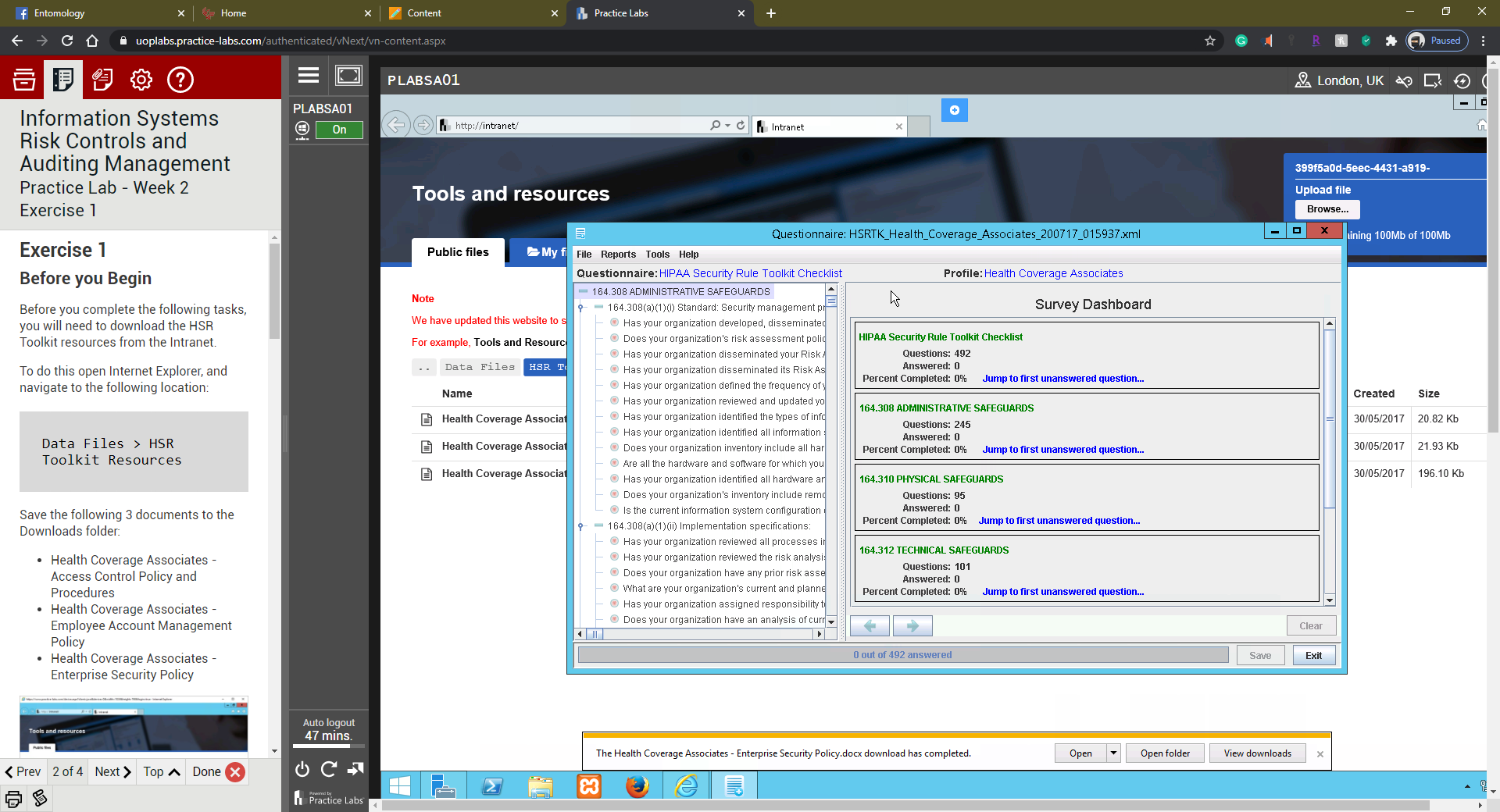
Choose **Standard Survey**and Click **OK**



#### Step 3

Click on **Use Survey**to complete this step. The list of questions (security controls) should appear.





## Exercise 2

### Task 1: Answer and Populate Risk Management Administrative Questions (Question #1)

#### Step 1

Navigate to 164.308 ADMINISTRATIVE SAFEGUARDS under Risk Management (164.308(a)(1)(ii)(B) and answer the question: Does your organization have policies and procedures in place for security?



#### Step 2

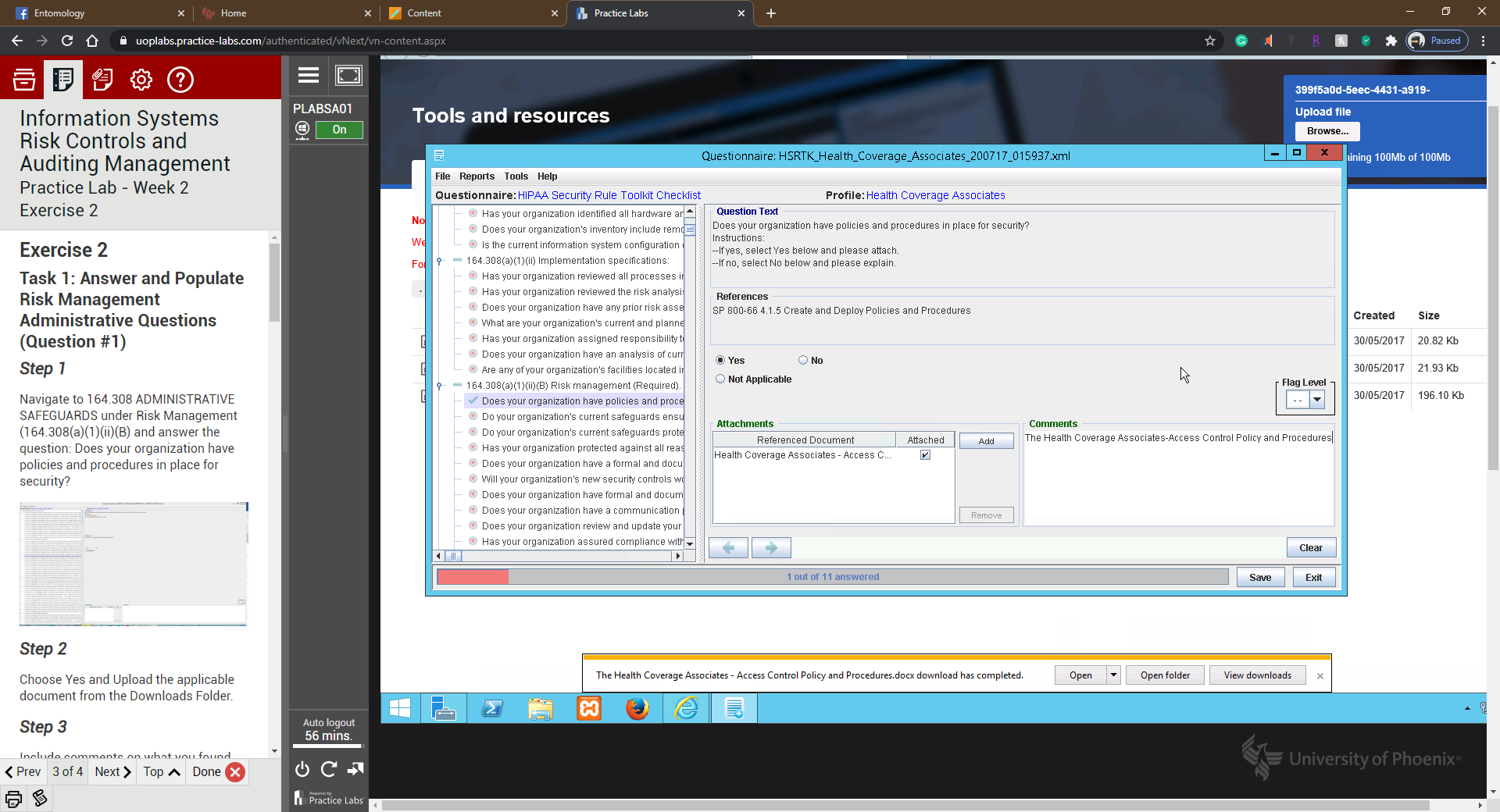
Choose Yes and Upload the applicable document from the Downloads Folder.

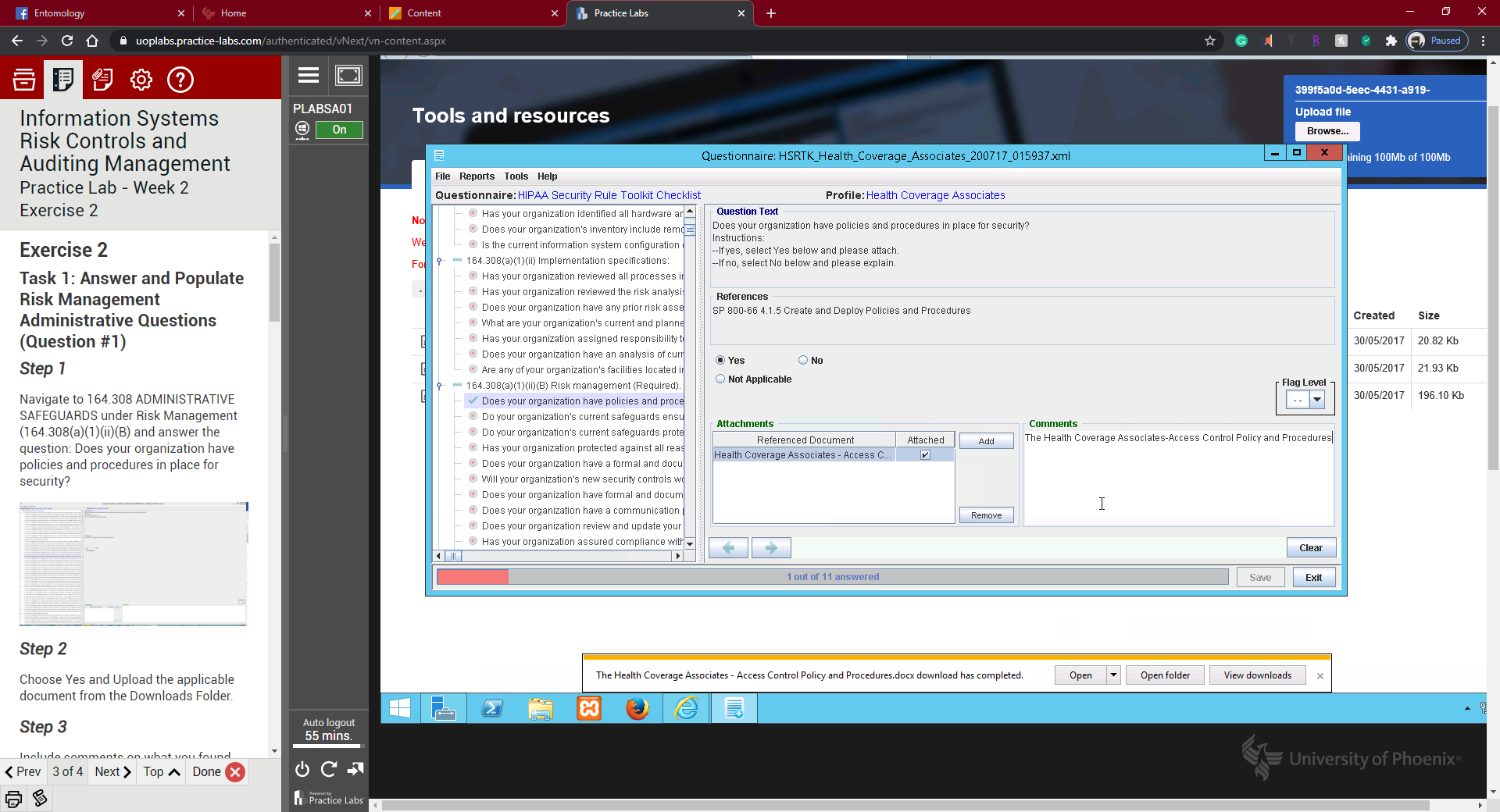
#### Step 3

Include comments on what you found after reviewing this question.

#### Step 4

Capture a screen shot of the uploaded document that you have chosen.

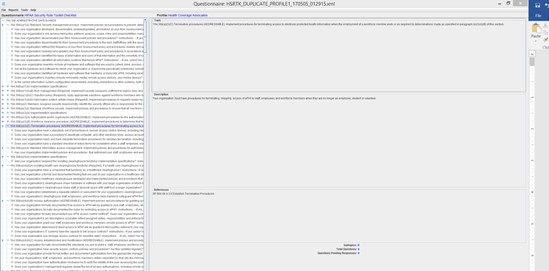




### Task 2: Answer and Populate Security Policy Questions (Question #2)

#### Step 1

Navigate to 164.308 ADMINISTRATIVE SAFEGUARDS under Termination Procedures (164.308(a)(3)(C) and answer the question: Does your organization implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a((3)(ii)(B) of this section?



#### Step 2

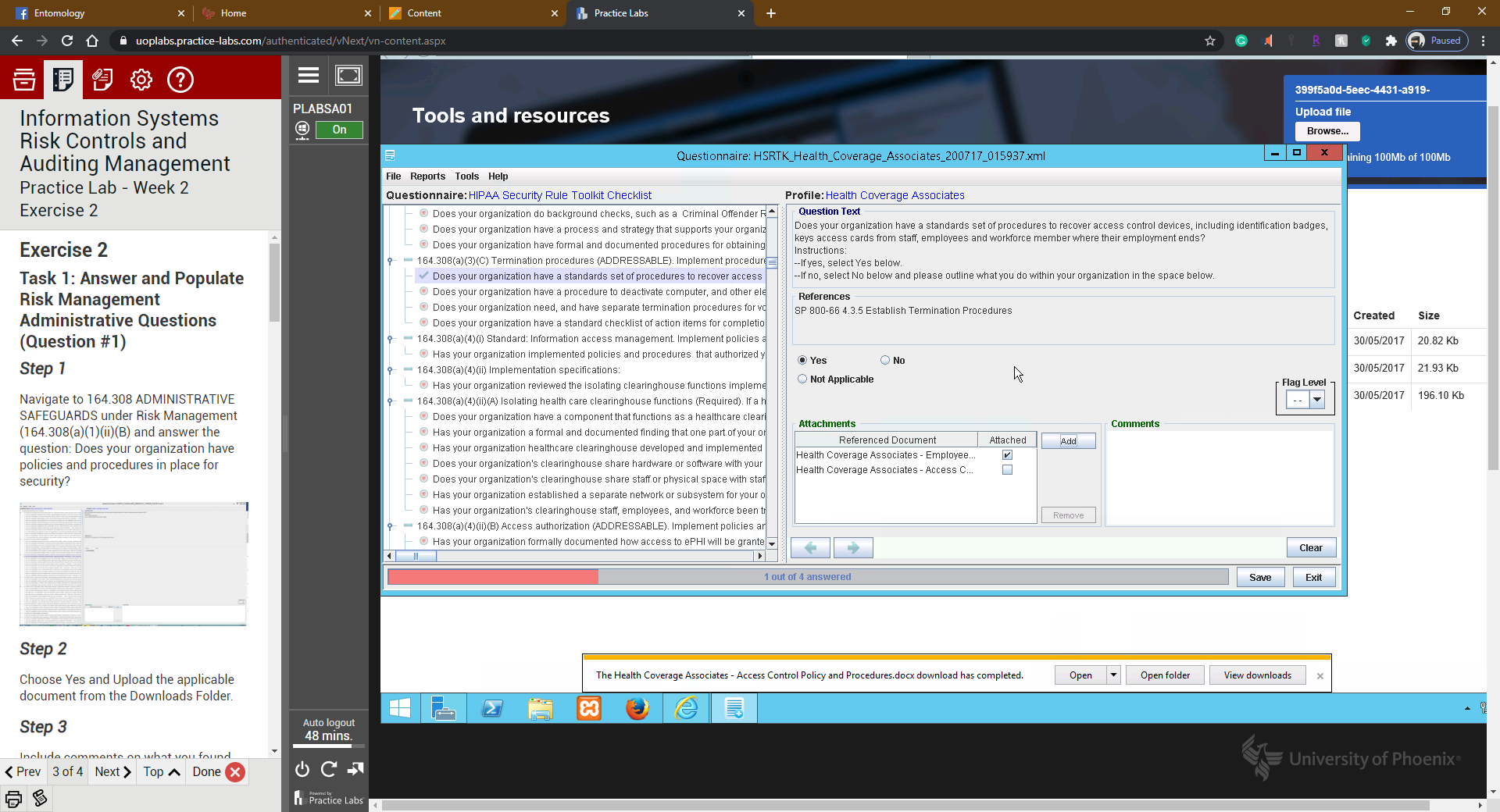
Choose Yes and Upload the applicable document from the Downloads Folder.

#### Step 3

Include comments on what you found after reviewing this question.

#### Step 4

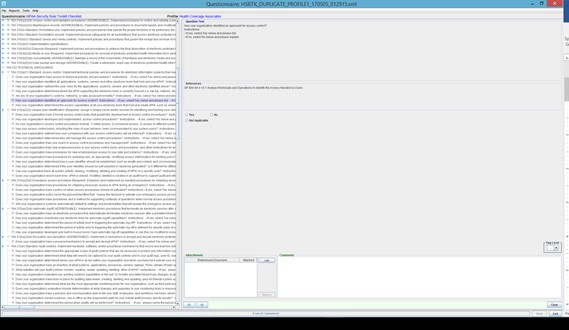
Capture a screen shot of the uploaded document that you have chosen.



### Task 3: Answer and Populate Technical Safeguard Questions (Question #3)

#### Step 1

Navigate to 164.312 TECHNICAL SAFEGUARDS under Access Control (164.312(a)(1) and answer the question: Has your organization identified an approach for access control? If so, how would it identify who requires access to PHI and who is not authorized access to PHI?



#### Step 2

Choose Yes and Upload the applicable document from the Downloads Folder.

#### Step 3

Include comments on what you found after reviewing this question.

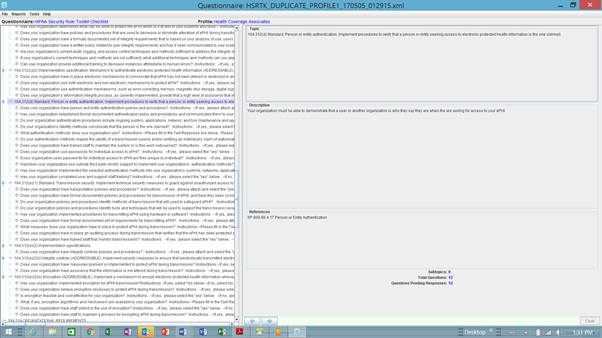
#### Step 4

Capture a screen shot of the uploaded document that you have chosen.

### Task 4: Answer and Populate Technical Safeguard Questions (Question #4)

#### Step 1

Navigate to 164.312 TECHNICAL SAFEGUARDS under Access Control (164.312(d) and answer the question: Has your implemented procedures to verify that a person or entity seeking access to electronic PHI is the one claimed? Is there a password stringency policy?



#### Step 2

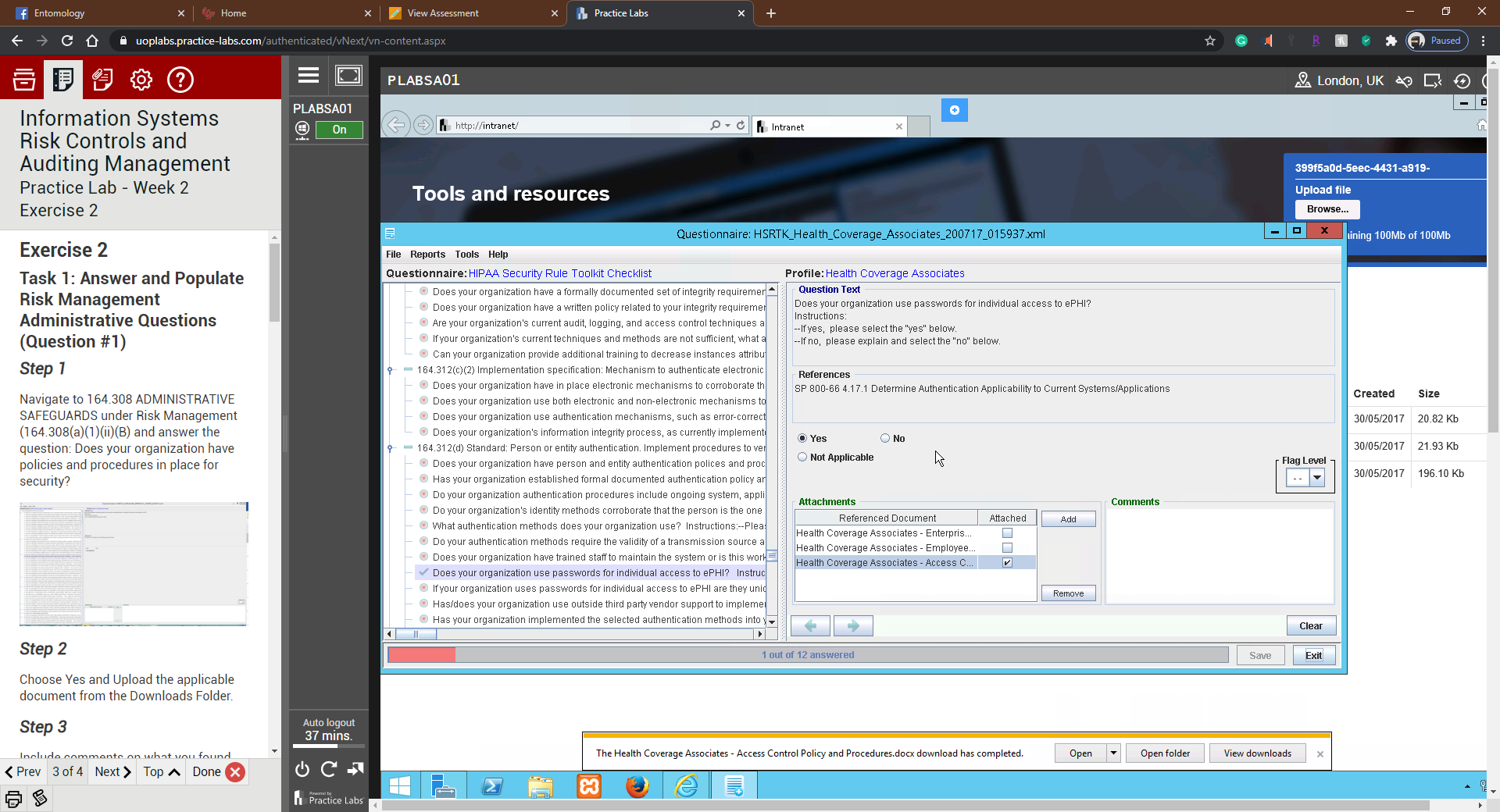
Choose Yes and Upload the applicable document from the Downloads Folder. Choose No if password stringency policy is not found. If it is not found, then weak passwords are more than likely being used (Reference Vulnerability #3 in this assignment).

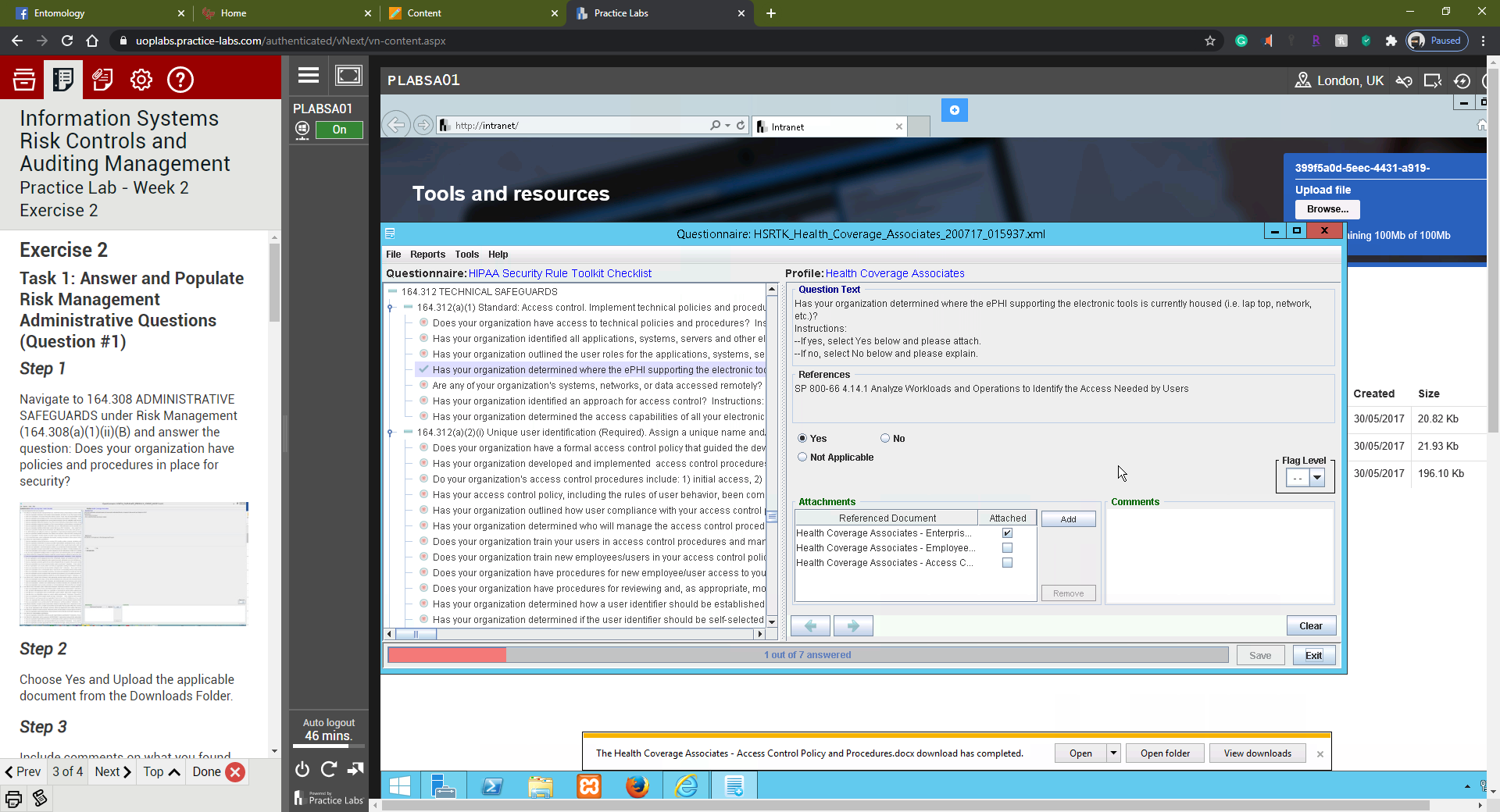
#### Step 3

Include comments on what you found after reviewing this question.

#### Step 4

Capture a screen shot of the uploaded document that you have chosen.

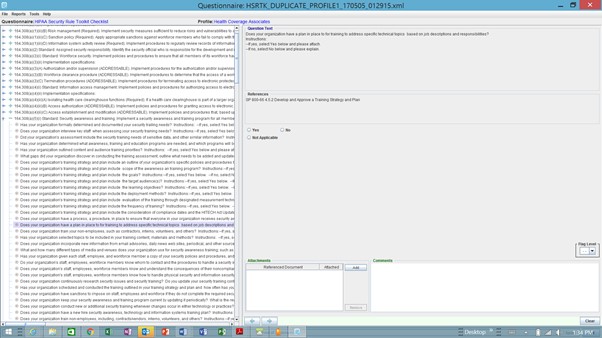




### Task 5: Answer and Populate Organizational Safeguard Questions (Question #5)

#### Step 1

Navigate to 164.308 ADMINISTRATIVE SAFEGUARDS under Security Awareness and Training (164.308(a)(5)(i) and answer the question: Does your organization have a policy or procedures in place for training for specific technical topics such as proper email communication, especially with respect to emailing and PHI (reference Vulnerability #2 in this assignment)?



#### Step 2

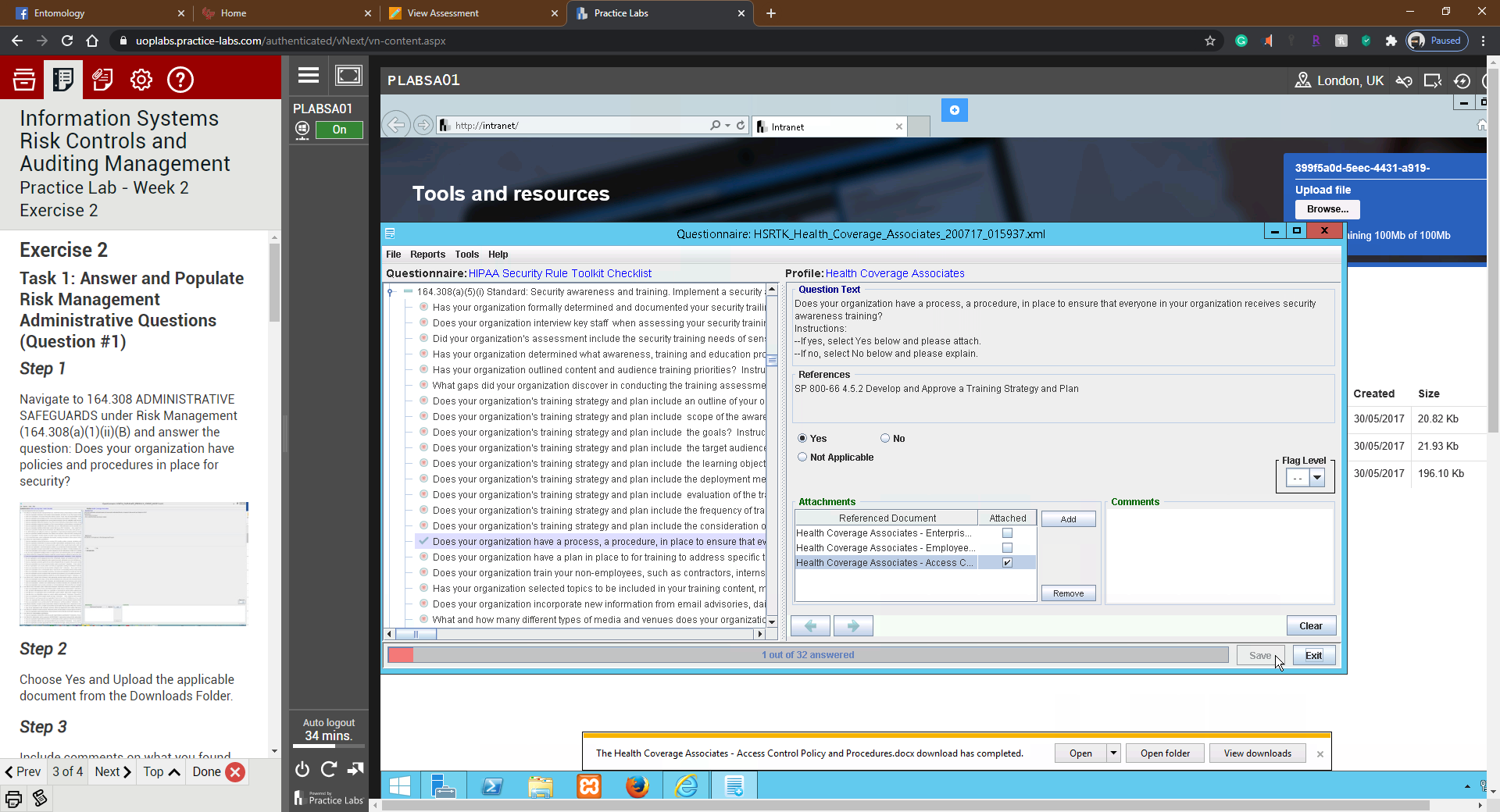
Choose Yes and Upload the applicable document from the Downloads Folder. Choose No if specific training documents with respect to email and PHI is not found. If it is not found, then weak passwords are more than likely being used (Reference Vulnerability #2 in this assignment).

#### Step 3

Include comments on what you found after reviewing this question.

#### Step 4

Capture a screen shot of the uploaded document that you have chosen.



**Summary**

You covered the following activities in this module:

* Incorporated the NIST HIPAA Security Toolkit Application, developed by the National Institute of Standards and Technology (NIST), to help your client:

1. Better understand the requirements of the HIPAA Security Rule,
2. Implement those requirements, and
3. Assess those implementations within in their operational environment.

* Answered a small sample set of questions the relate to the vulnerabilities as described in the assignment.
* Uploaded the related artifacts (documents) as proof of compliance.
* Summarized how the selected controls (questions) help mitigate the risks associated with the vulnerabilities.