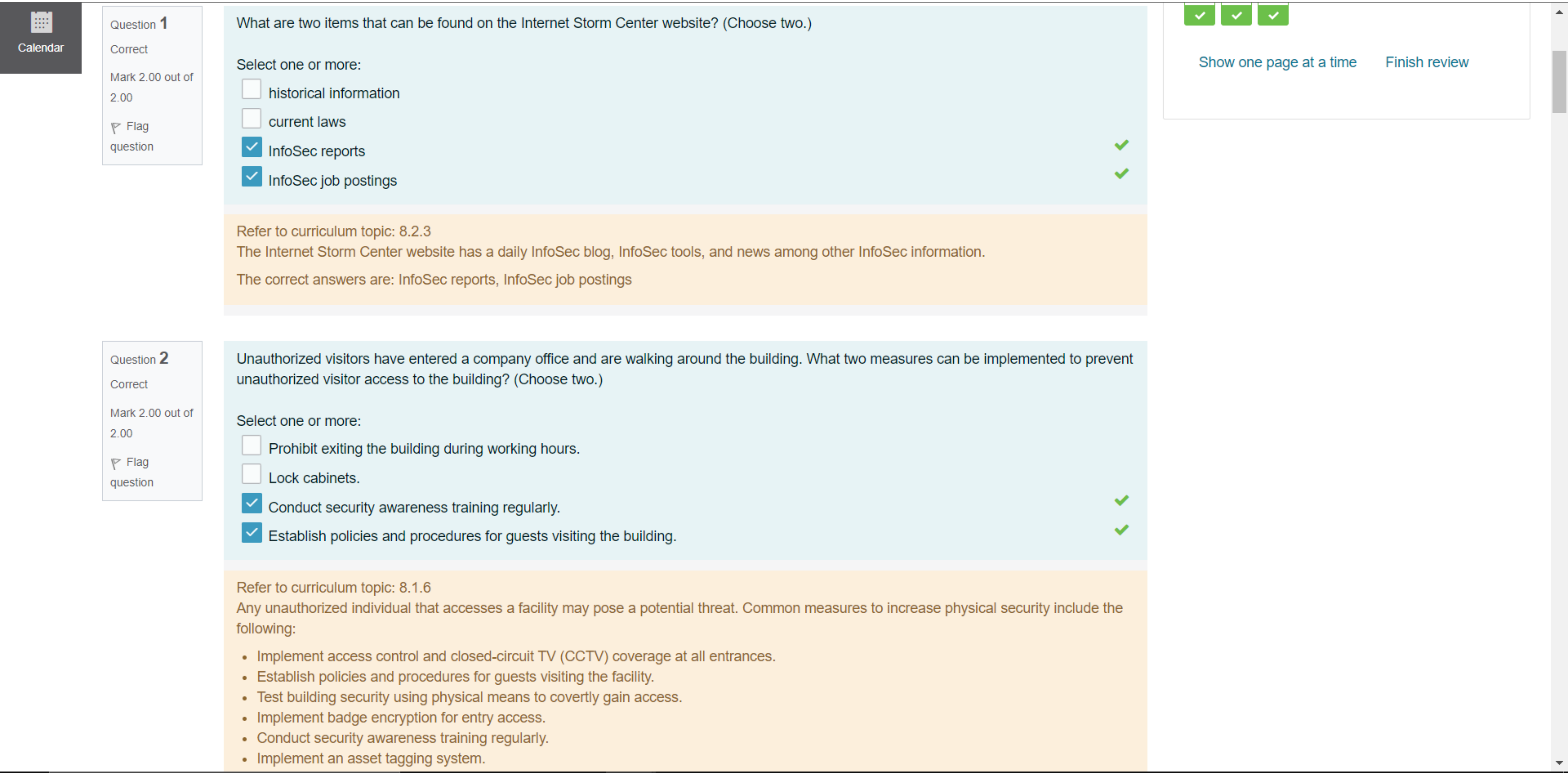


Question 1

Correct

Mark 2.00 out of 2.00

Flag question

What are two items that can be found on the Internet Storm Center website? (Choose two.)

Select one or more:

☐ historical information

☐ current laws

☑ InfoSec reports ✓

☑ InfoSec job postings ✓

Refer to curriculum topic: 8.2.3
The Internet Storm Center website has a daily InfoSec blog, InfoSec tools, and news among other InfoSec information.

The correct answers are: InfoSec reports, InfoSec job postings

Question 2

Correct

Mark 2.00 out of 2.00

Flag question

Unauthorized visitors have entered a company office and are walking around the building. What two measures can be implemented to prevent unauthorized visitor access to the building? (Choose two.)

Select one or more:

☐ Prohibit exiting the building during working hours.

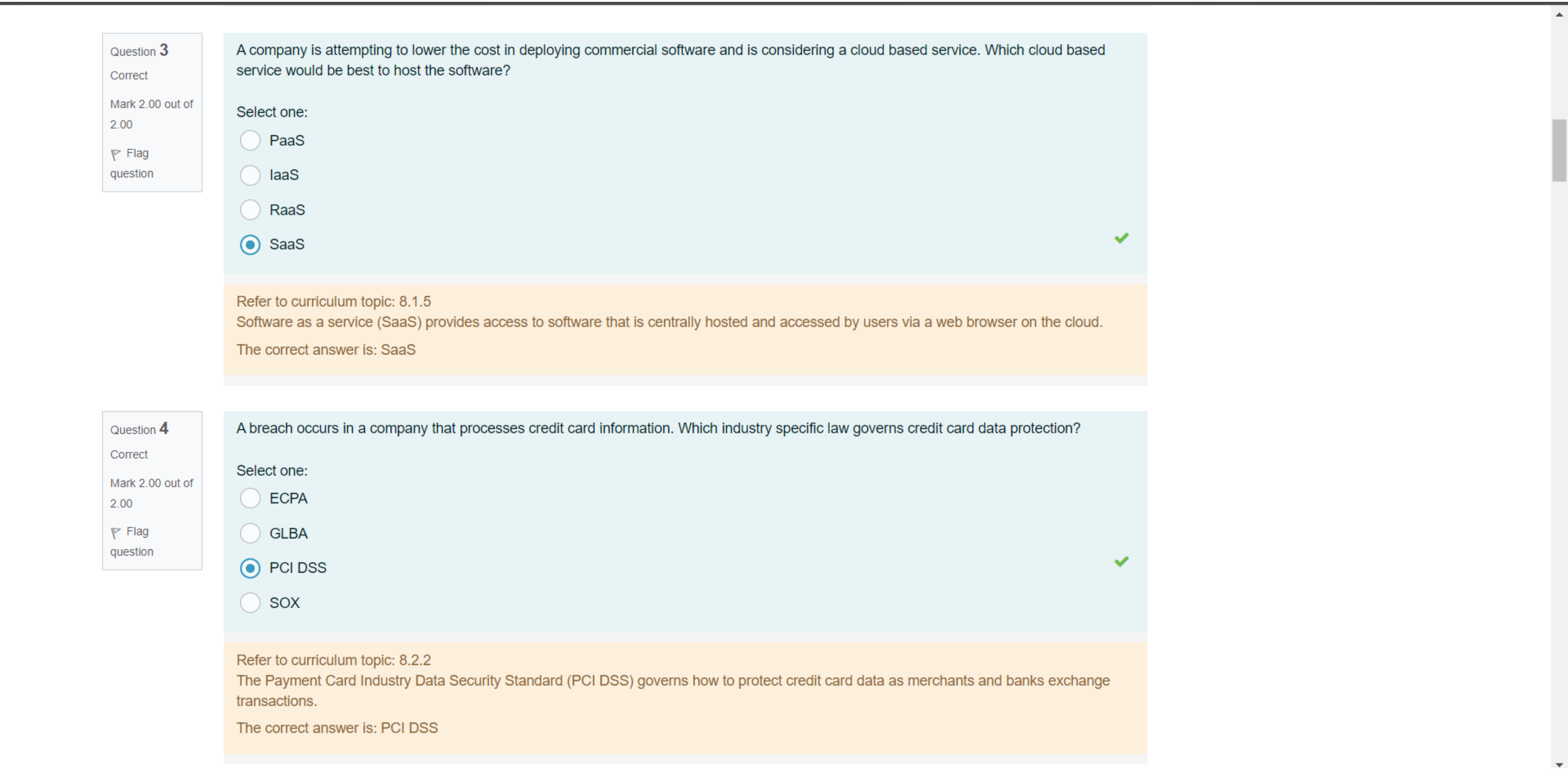
☐ Lock cabinets.

☑ Conduct security awareness training regularly. ✓

☑ Establish policies and procedures for guests visiting the building. ✓

Refer to curriculum topic: 8.1.6
Any unauthorized individual that accesses a facility may pose a potential threat. Common measures to increase physical security include the following:

- Implement access control and closed-circuit TV (CCTV) coverage at all entrances.
- Establish policies and procedures for guests visiting the facility.
- Test building security using physical means to covertly gain access.
- Implement badge encryption for entry access.
- Conduct security awareness training regularly.
- Implement an asset tagging system.



Question **3**

Correct

Mark 2.00 out of 2.00

A company is attempting to lower the cost in deploying commercial software and is considering a cloud based service. Which cloud based service would be best to host the software?

Select one:

○ PaaS

○ IaaS

○ RaaS

● SaaS ✓

Refer to curriculum topic: 8.1.5
Software as a service (SaaS) provides access to software that is centrally hosted and accessed by users via a web browser on the cloud.

The correct answer is: SaaS

Question **4**

Correct

Mark 2.00 out of 2.00

A breach occurs in a company that processes credit card information. Which industry specific law governs credit card data protection?

Select one:

○ ECPA

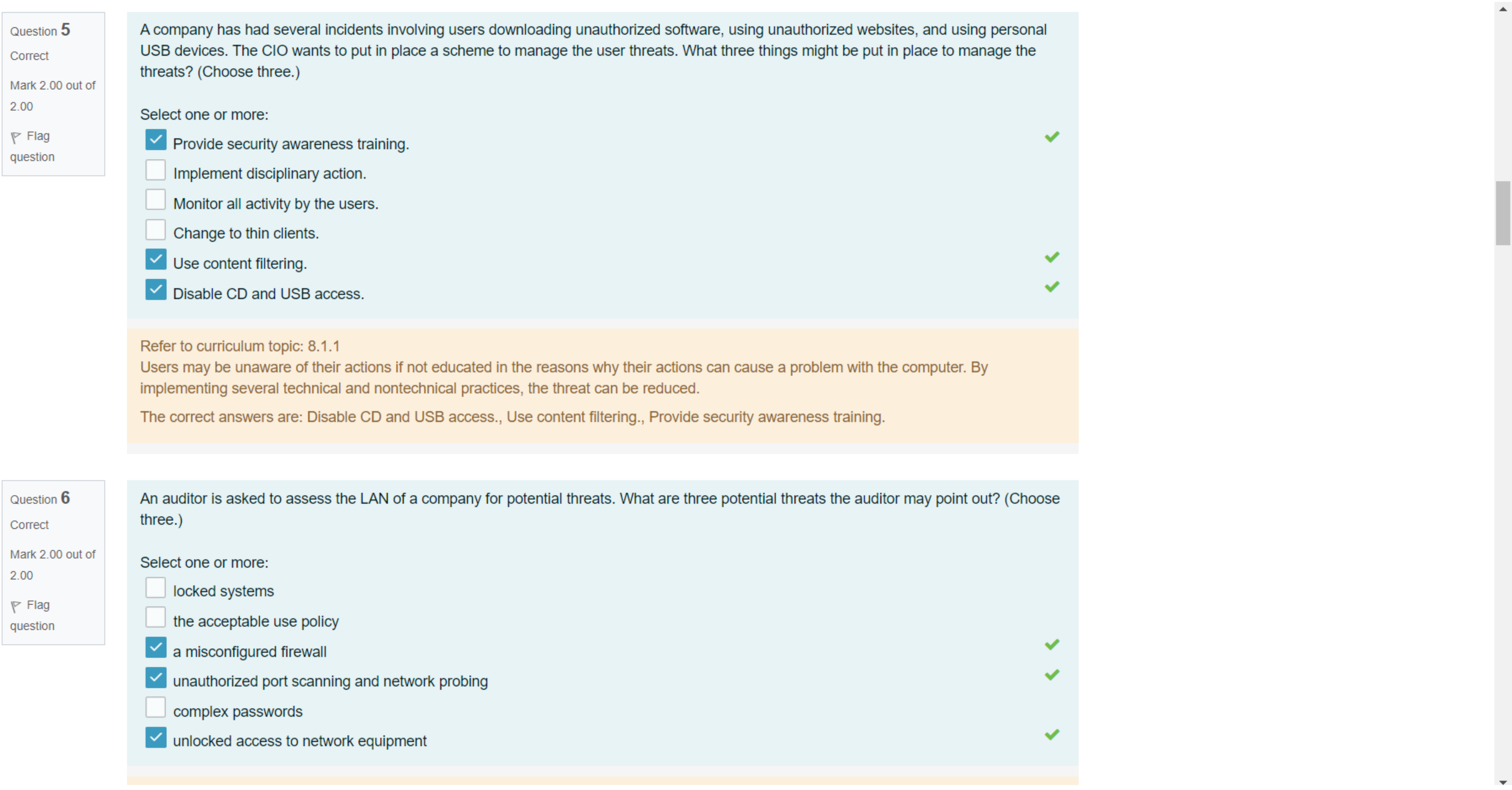
○ GLBA

● PCI DSS ✓

○ SOX

Refer to curriculum topic: 8.2.2
The Payment Card Industry Data Security Standard (PCI DSS) governs how to protect credit card data as merchants and banks exchange transactions.

The correct answer is: PCI DSS



Question 5

Correct

Mark 2.00 out of 2.00

Flag question

A company has had several incidents involving users downloading unauthorized software, using unauthorized websites, and using personal USB devices. The CIO wants to put in place a scheme to manage the user threats. What three things might be put in place to manage the threats? (Choose three.)

Select one or more:

☑ Provide security awareness training. ✓

□ Implement disciplinary action.

□ Monitor all activity by the users.

□ Change to thin clients.

☑ Use content filtering. ✓

☑ Disable CD and USB access. ✓

Refer to curriculum topic: 8.1.1
Users may be unaware of their actions if not educated in the reasons why their actions can cause a problem with the computer. By implementing several technical and nontechnical practices, the threat can be reduced.

The correct answers are: Disable CD and USB access., Use content filtering., Provide security awareness training.

Question 6

Correct

Mark 2.00 out of 2.00

Flag question

An auditor is asked to assess the LAN of a company for potential threats. What are three potential threats the auditor may point out? (Choose three.)

Select one or more:

□ locked systems

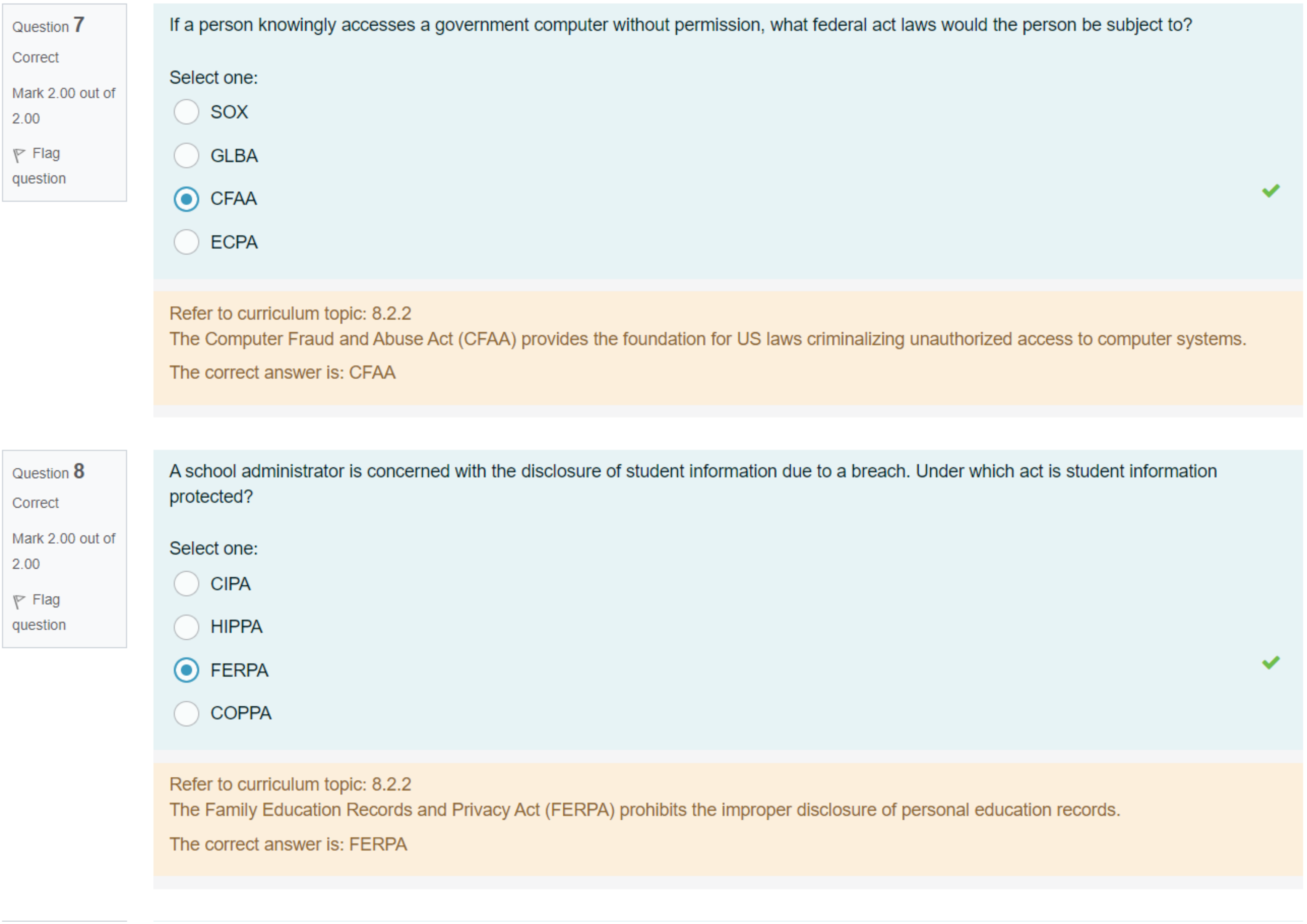
□ the acceptable use policy

☑ a misconfigured firewall ✓

☑ unauthorized port scanning and network probing ✓

□ complex passwords

☑ unlocked access to network equipment ✓



Question **7**

Correct

Mark 2.00 out of 2.00

Flag question

If a person knowingly accesses a government computer without permission, what federal act laws would the person be subject to?

Select one:

○ SOX

○ GLBA

● CFAA ✓

○ ECPA

Refer to curriculum topic: 8.2.2
The Computer Fraud and Abuse Act (CFAA) provides the foundation for US laws criminalizing unauthorized access to computer systems.

The correct answer is: CFAA

Question **8**

Correct

Mark 2.00 out of 2.00

Flag question

A school administrator is concerned with the disclosure of student information due to a breach. Under which act is student information protected?

Select one:

○ CIPA

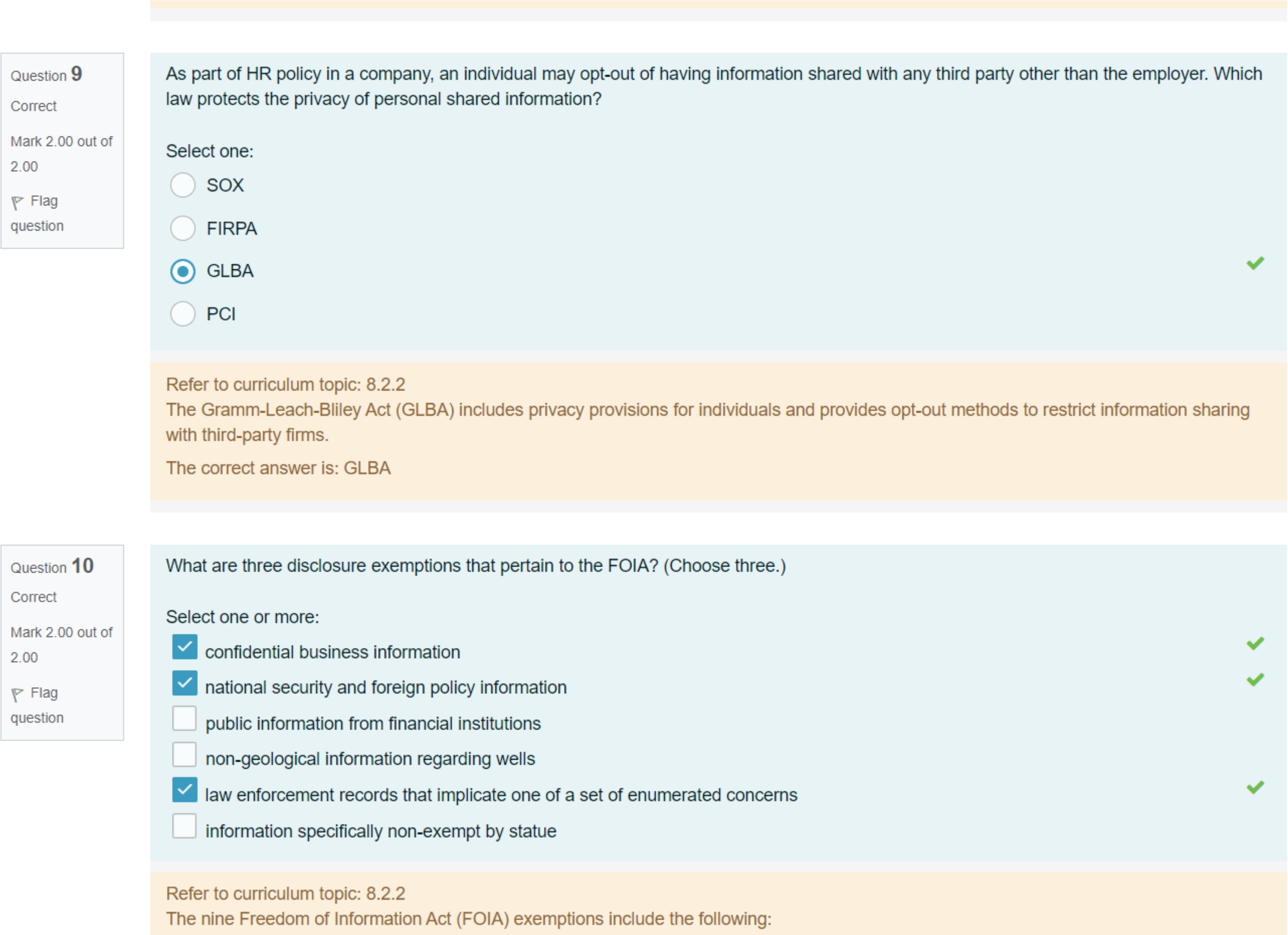
○ HIPPA

● FERPA ✓

○ COPPA

Refer to curriculum topic: 8.2.2
The Family Education Records and Privacy Act (FERPA) prohibits the improper disclosure of personal education records.

The correct answer is: FERPA



Question **9**

Correct

Mark 2.00 out of 2.00

Flag question

As part of HR policy in a company, an individual may opt-out of having information shared with any third party other than the employer. Which law protects the privacy of personal shared information?

Select one:

○ SOX

○ FIRPA

● GLBA ✓

○ PCI

Refer to curriculum topic: 8.2.2
The Gramm-Leach-Bliley Act (GLBA) includes privacy provisions for individuals and provides opt-out methods to restrict information sharing with third-party firms.

The correct answer is: GLBA

Question **10**

Correct

Mark 2.00 out of 2.00

Flag question

What are three disclosure exemptions that pertain to the FOIA? (Choose three.)

Select one or more:

☑ confidential business information ✓

☑ national security and foreign policy information ✓

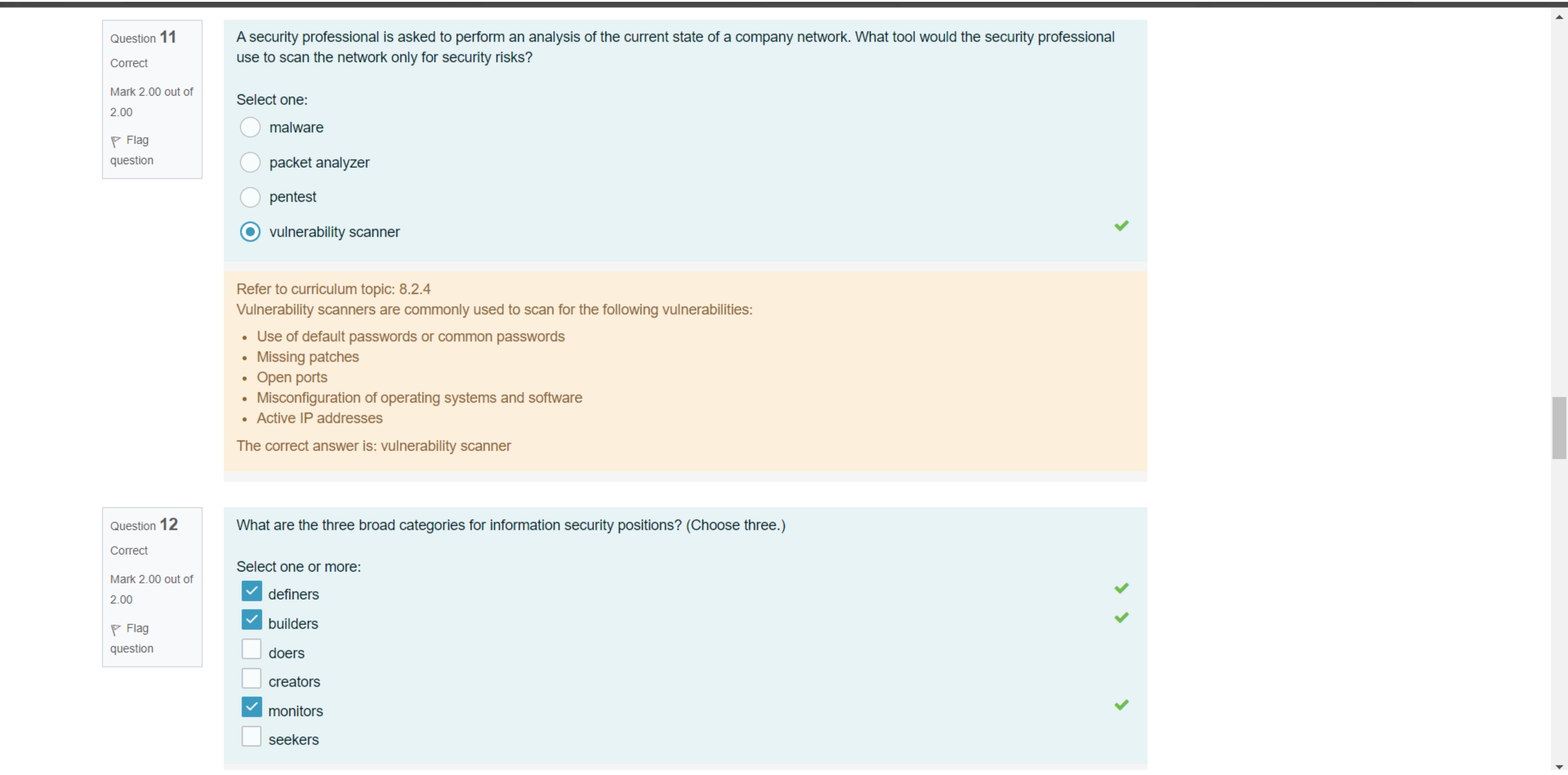
□ public information from financial institutions

□ non-geological information regarding wells

☑ law enforcement records that implicate one of a set of enumerated concerns ✓

□ information specifically non-exempt by statue

Refer to curriculum topic: 8.2.2
The nine Freedom of Information Act (FOIA) exemptions include the following:



Question **11**

Correct

Mark 2.00 out of 2.00

Flag question

A security professional is asked to perform an analysis of the current state of a company network. What tool would the security professional use to scan the network only for security risks?

Select one:

○ malware

○ packet analyzer

○ pentest

● vulnerability scanner ✓

Refer to curriculum topic: 8.2.4
Vulnerability scanners are commonly used to scan for the following vulnerabilities:

- Use of default passwords or common passwords
- Missing patches
- Open ports
- Misconfiguration of operating systems and software
- Active IP addresses

The correct answer is: vulnerability scanner

Question **12**

Correct

Mark 2.00 out of 2.00

Flag question

What are the three broad categories for information security positions? (Choose three.)

Select one or more:

☑ definers ✓

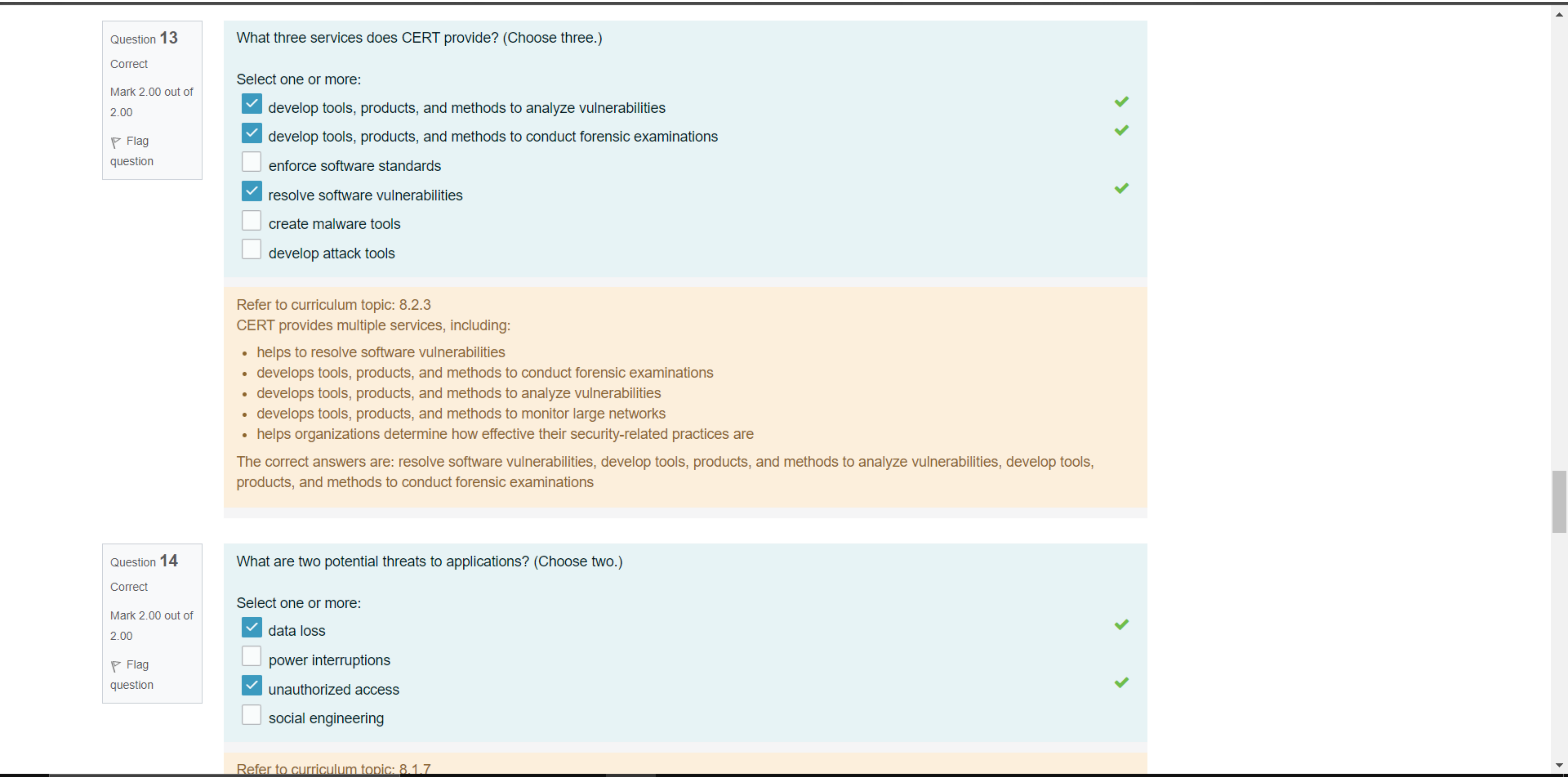
☑ builders ✓

☐ doers

☐ creators

☑ monitors ✓

☐ seekers



Question **13**

Correct

Mark 2.00 out of 2.00

Flag question

What three services does CERT provide? (Choose three.)

Select one or more:

- ☑ develop tools, products, and methods to analyze vulnerabilities ✓
- ☑ develop tools, products, and methods to conduct forensic examinations ✓
- □ enforce software standards
- ☑ resolve software vulnerabilities ✓
- □ create malware tools
- □ develop attack tools

Refer to curriculum topic: 8.2.3
CERT provides multiple services, including:

- helps to resolve software vulnerabilities
- develops tools, products, and methods to conduct forensic examinations
- develops tools, products, and methods to analyze vulnerabilities
- develops tools, products, and methods to monitor large networks
- helps organizations determine how effective their security-related practices are

The correct answers are: resolve software vulnerabilities, develop tools, products, and methods to analyze vulnerabilities, develop tools, products, and methods to conduct forensic examinations

Question **14**

Correct

Mark 2.00 out of 2.00

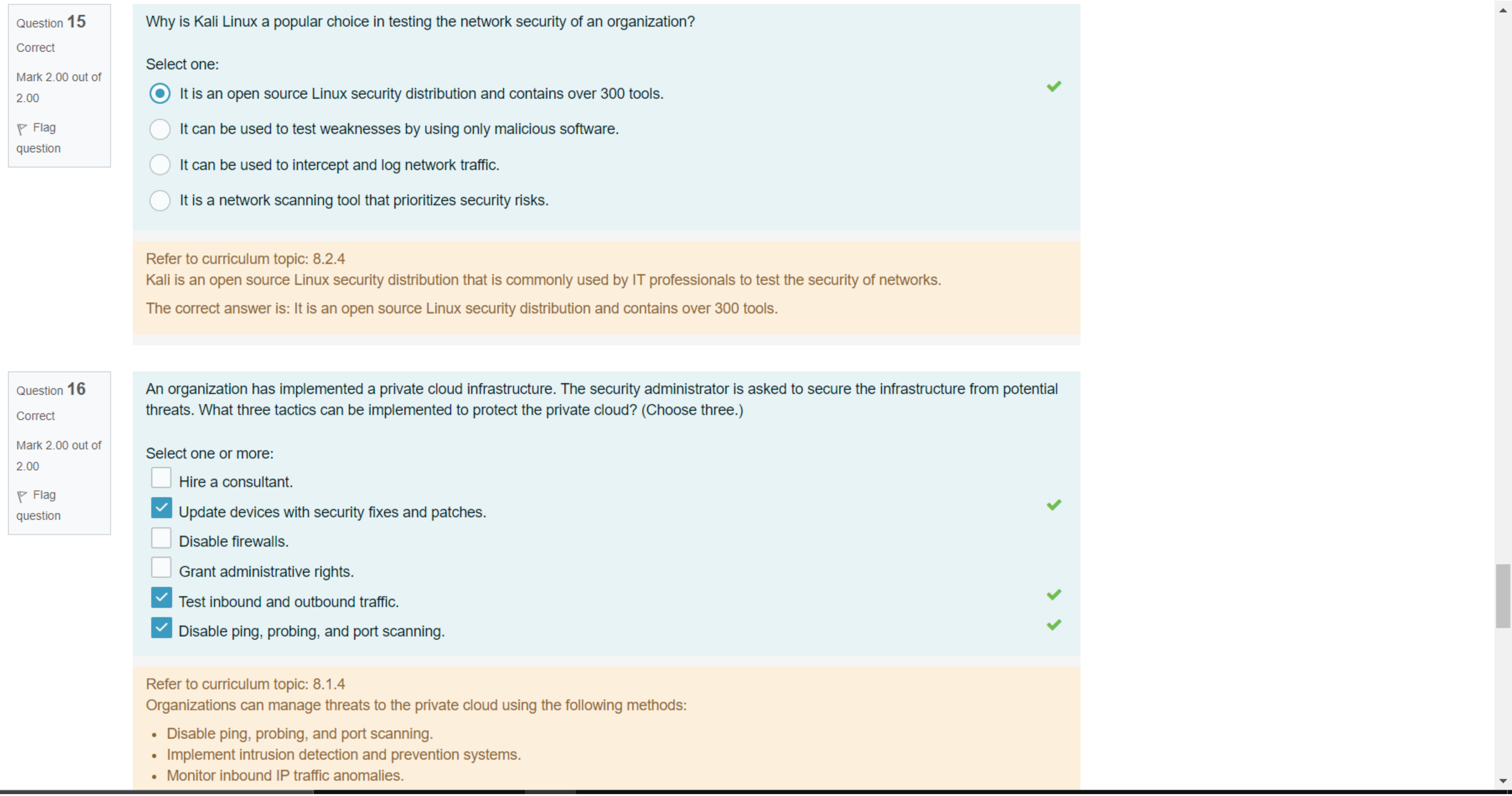
Flag question

What are two potential threats to applications? (Choose two.)

Select one or more:

- ☑ data loss ✓
- □ power interruptions
- ☑ unauthorized access ✓
- □ social engineering

Refer to curriculum topic: 8.1.7



Question **15**

Correct

Mark 2.00 out of 2.00

Flag question

Why is Kali Linux a popular choice in testing the network security of an organization?

Select one:

● It is an open source Linux security distribution and contains over 300 tools. ✓

○ It can be used to test weaknesses by using only malicious software.

○ It can be used to intercept and log network traffic.

○ It is a network scanning tool that prioritizes security risks.

Refer to curriculum topic: 8.2.4
Kali is an open source Linux security distribution that is commonly used by IT professionals to test the security of networks.

The correct answer is: It is an open source Linux security distribution and contains over 300 tools.

Question **16**

Correct

Mark 2.00 out of 2.00

Flag question

An organization has implemented a private cloud infrastructure. The security administrator is asked to secure the infrastructure from potential threats. What three tactics can be implemented to protect the private cloud? (Choose three.)

Select one or more:

□ Hire a consultant.

☑ Update devices with security fixes and patches. ✓

□ Disable firewalls.

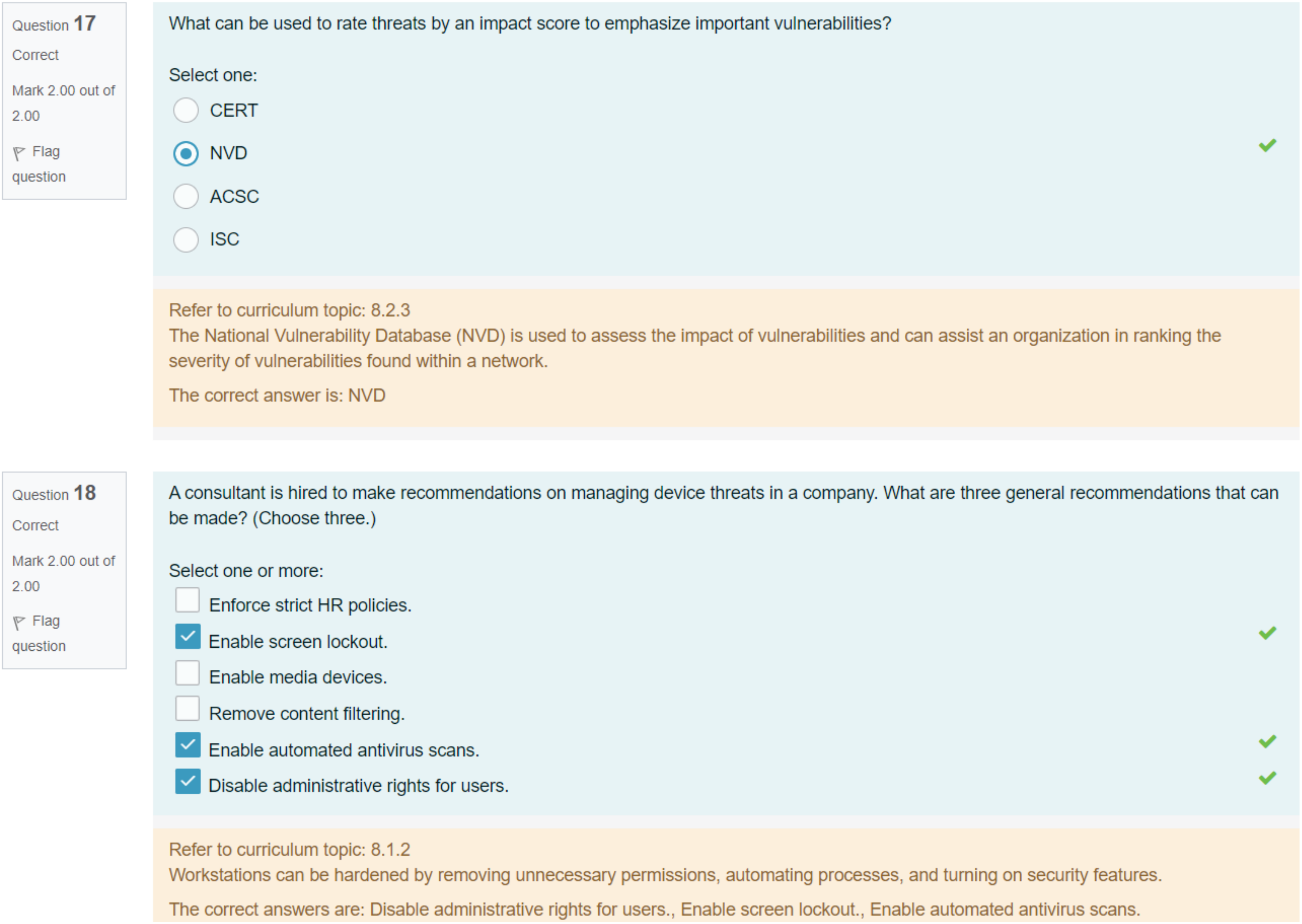
□ Grant administrative rights.

☑ Test inbound and outbound traffic. ✓

☑ Disable ping, probing, and port scanning. ✓

Refer to curriculum topic: 8.1.4
Organizations can manage threats to the private cloud using the following methods:

- Disable ping, probing, and port scanning.
- Implement intrusion detection and prevention systems.
- Monitor inbound IP traffic anomalies.



Question **17**

Correct

Mark 2.00 out of 2.00

Flag question

What can be used to rate threats by an impact score to emphasize important vulnerabilities?

Select one:

○ CERT

● NVD ✓

○ ACSC

○ ISC

Refer to curriculum topic: 8.2.3
The National Vulnerability Database (NVD) is used to assess the impact of vulnerabilities and can assist an organization in ranking the severity of vulnerabilities found within a network.

The correct answer is: NVD

Question **18**

Correct

Mark 2.00 out of 2.00

Flag question

A consultant is hired to make recommendations on managing device threats in a company. What are three general recommendations that can be made? (Choose three.)

Select one or more:

☐ Enforce strict HR policies.

☑ Enable screen lockout. ✓

☐ Enable media devices.

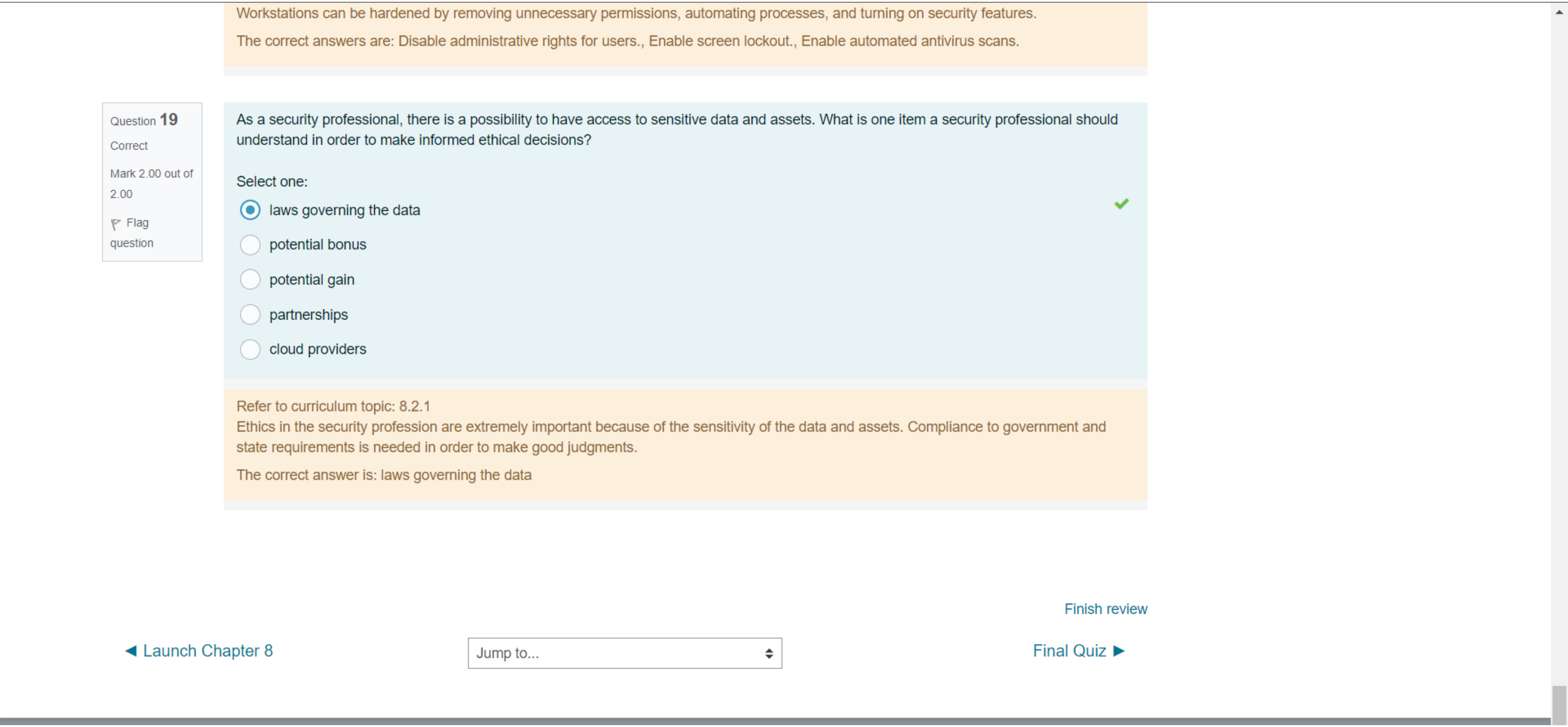
☐ Remove content filtering.

☑ Enable automated antivirus scans. ✓

☑ Disable administrative rights for users. ✓

Refer to curriculum topic: 8.1.2
Workstations can be hardened by removing unnecessary permissions, automating processes, and turning on security features.

The correct answers are: Disable administrative rights for users., Enable screen lockout., Enable automated antivirus scans.



Workstations can be hardened by removing unnecessary permissions, automating processes, and turning on security features.

The correct answers are: Disable administrative rights for users., Enable screen lockout., Enable automated antivirus scans.

Question **19**

Correct

Mark 2.00 out of 2.00

As a security professional, there is a possibility to have access to sensitive data and assets. What is one item a security professional should understand in order to make informed ethical decisions?

Select one:

● laws governing the data ✓

○ potential bonus

○ potential gain

○ partnerships

○ cloud providers

Refer to curriculum topic: 8.2.1
Ethics in the security profession are extremely important because of the sensitivity of the data and assets. Compliance to government and state requirements is needed in order to make good judgments.

The correct answer is: laws governing the data