

Four scoping questions practitioners get wrong

PCI DSS, the EU AI Act, HIPAA and CMMC. Four real questions, answered from the text of each standard, with an eight-question check and a completion record.

FORMAT

Self-study reading and quiz

TIME

About 1 hour

LEVEL

Intermediate

AUTHOR

Edward Casteloes CISSP, CISA

About CPE credit. These notes are designed as about one hour of self-study. Whether they count toward your continuing professional education, and how many hours you may claim, is set by your certifying body (for example ISC2 or ISACA). Check its current CPE policy before you report the hours, and keep this document and your completed record as evidence.

How to use these notes

1. Read each module: the question, what the text says, and the common mistake.
2. Answer the eight questions on the quiz page without looking back.
3. Check your answers against the key, then fill in the completion record on the last page.

■ MODULE 1 • PCI DSS V4.0.1

Learning objective. Decide when an embedded payment iframe keeps a merchant on SAQ A, and what SAQ A still requires.

THE QUESTION

Our checkout embeds our payment processor's iframe, loaded directly from the processor. Can we use SAQ A, and do we still need ASV scans?

What the text says

- SAQ A fits when every element of the payment page comes only and directly from a PCI DSS compliant third-party service provider, by redirect or by an iframe loaded directly from that provider, and no merchant system electronically touches card data.
- If any element comes from, or could be altered by, the merchant's own site (direct post, merchant-hosted fields, a proxied or self-served script), the merchant moves to SAQ A-EP.
- The January 2025 revision of SAQ A (r1) removed Requirements 6.4.3, 11.6.1 and 12.3.1 as line items and added an eligibility statement: the merchant's site is not susceptible to script attacks that could affect its e-commerce systems.
- That statement matters for merchants that embed a provider's form, not for plain redirects. It can be supported by script protections on the embedding page, or by confirmation from the processor that its iframe protects against script attacks when implemented as instructed.
- Quarterly external vulnerability scans by a PCI SSC Approved Scanning Vendor (Requirement 11.3.2) still apply on SAQ A for redirect and iframe merchants.
- The acquirer has the final say on which SAQ a merchant may use.

Common mistake. Treating "we outsourced the payment form" as "we have no PCI DSS obligations". The ASV scans remain, and the script-attack statement needs evidence behind it.

Full answer with citations: compliancecolleague.ai/answers/pci-dss-saq-a-iframe-asv-scans?ref=cpe

Learning objective. State the application dates for high-risk obligations after the Digital Omnibus, and apply the transitional rule for systems already on the market.

THE QUESTION

When do the EU AI Act high-risk obligations apply to Annex III systems such as CV-screening tools, and to Annex I product safety components?

What the text says

- Annex III systems, such as CV-screening tools (Annex III point 4(a)): the Chapter III, Sections 1 to 3 obligations apply from 2 December 2027 (Article 113, as amended by Regulation (EU) 2026/1744). The original date was 2 August 2026.
- Annex I systems (safety components of products that need third-party conformity assessment, such as machinery or medical devices): from 2 August 2028.
- Article 111(2), as replaced by Regulation (EU) 2026/1744: a high-risk system placed on the market or put into service before its application date is caught only if it undergoes a significant design change on or after that date. This is a grace period, not an exemption.
- A significant change made before the application date does not start the obligations early.
- Systems intended for use by public authorities must comply by 2 August 2030, whether or not they change.
- The grace period does not touch Article 5 (prohibited practices) or the Article 50 transparency duties, which run on their own timelines.
- A system first placed on the market after the application date gets no grace period.

Common mistake. Assuming a legacy tool is exempt for good. Any significant design change on or after the application date brings the full obligations, including conformity assessment.

Full answer with citations: compliancecolleague.ai/answers/eu-ai-act-high-risk-application-dates?ref=cpe

■ MODULE 3 • HIPAA

Learning objective. Apply the business associate definition and the conduit exception to a vendor that stores encrypted ePHI.

THE QUESTION

We're a SaaS vendor that stores a hospital's ePHI in encrypted form and never views it. Are we a HIPAA business associate?

What the text says

- Yes. The definition of business associate in 45 CFR § 160.103 covers anyone who creates, receives, maintains or transmits PHI on behalf of a covered entity. Storing encrypted ePHI is maintaining it.
- The conduit exception covers mere transmission on a transient basis, such as a telecom carrier, where any storage is incidental. It does not cover storage services.
- HHS guidance on HIPAA and cloud computing says a cloud provider that stores only encrypted ePHI and lacks the key is still a business associate.
- The covered entity needs satisfactory assurances in a written business associate agreement (§ 164.502(e)(1) and § 164.308(b)(1)).
- The business associate is directly subject to most of the Security Rule (§§ 164.308, 164.310, 164.312) and must notify the covered entity of a breach of unsecured PHI without unreasonable delay and no later than 60 days after discovery (§ 164.410).
- A zero-knowledge design can lower risk and may feature in the § 164.402 breach risk assessment, but it does not remove business associate status.

Common mistake. Relying on "we never see the data". Encryption without the key changes the risk, not the role.

Full answer with citations: compliancecolleague.ai/answers/hipaa-encrypted-storage-business-associate?ref=cpe

■ MODULE 4 • CMMC (32 CFR PART 170)

Learning objective. Classify security tools and providers under the CMMC asset categories in 32 CFR 170.19.

THE QUESTION

Our SIEM and MFA provider don't store or process CUI. Are they in scope for our CMMC Level 2 assessment?

What the text says

- Not storing or processing CUI does not take a tool out of scope. What matters is whether it performs a security function for the CUI environment.
- A SIEM or MFA service the contractor runs itself is a Security Protection Asset (table 3 to § 170.19(c)(1)). It is assessed for the security capability it provides, and must be in the asset inventory, the SSP and the network diagram.
- A provider that delivers the service and handles only Security Protection Data (log data, configuration data and the like, defined in § 170.2), without CUI, is an External Service Provider (table 4 to § 170.19(c)(2)(i)). It stays in scope, and its services are assessed as Security Protection Assets.
- Each ESP relationship must be documented in the SSP with a service description and a customer responsibility matrix.
- A provider is out of scope only if it handles neither CUI nor Security Protection Data and has no security-relevant connection to CUI assets.
- A federal information system operated on the Government's behalf falls outside Part 170 altogether (§ 170.3(b)).

Common mistake. Leaving the SIEM and the identity provider off the boundary diagram because they hold no CUI. Assessors expect to see them, and to test the capability each provides.

Full answer with citations: compliancecolleague.ai/answers/cmmc-siem-mfa-assessment-scope?ref=cpe

■ KNOWLEDGE CHECK

Eight questions

Circle one answer for each question. The key is on the next page.

1. A merchant's checkout uses an iframe served directly from its PCI DSS compliant processor. No merchant system touches card data. Which SAQ normally applies?

- A SAQ A
- B SAQ A-EP
- C SAQ D for merchants
- D SAQ B-IP

2. The same merchant is on SAQ A. Which requirement still applies?

- A Annual penetration testing of the processor's iframe
- B Quarterly external scans by an Approved Scanning Vendor (11.3.2)
- C None: outsourcing removes all testing
- D Requirement 6.4.3 as a line item

3. From what date do the EU AI Act high-risk obligations apply to an Annex III CV-screening tool placed on the market in 2028?

- A 2 August 2026
- B 2 December 2027
- C 2 August 2028
- D 2 August 2030

4. A private company's CV-screening tool went on the market in January 2027 and has not changed since. When do the high-risk obligations reach it?

- A On 2 December 2027, automatically
- B Never: it is grandfathered
- C Only if it undergoes a significant design change on or after 2 December 2027
- D On 2 August 2030

5. A SaaS vendor stores a hospital's ePHI encrypted and holds no key. Under 45 CFR § 160.103, it is:

- A Exempt as a conduit
- B A business associate, because it maintains ePHI
- C Exempt if the encryption meets NIST guidance
- D A covered entity

6. What is the outer limit for a business associate to notify the covered entity of a breach of unsecured PHI?

- A 24 hours
- B 72 hours
- C 30 days
- D 60 days after discovery

7. A contractor's own SIEM collects logs from its CUI environment but stores no CUI. Under 32 CFR 170.19 it is:

- A Out of scope
- B A CUI Asset
- C A Security Protection Asset
- D A Specialized Asset

8. A managed security provider handles only the contractor's log and configuration data, never CUI. What follows?

- A It is out of scope because it handles no CUI
- B It is an External Service Provider in scope, documented in the SSP with a customer responsibility matrix
- C It must itself hold a CMMC Level 2 certificate before the assessment
- D It is assessed against all 110 practices

Answers and why

- 1. A** Payment page elements served only and directly from a compliant provider keep the merchant on SAQ A. The acquirer confirms final eligibility.
- 2. B** SAQ A keeps the external ASV scan requirement for redirect and iframe merchants. 6.4.3 was removed as a line item in SAQ A r1.
- 3. B** Annex III obligations apply from 2 December 2027 after Regulation (EU) 2026/1744. A system placed on the market after that date gets no grace period.
- 4. C** Article 111(2) gives a grace period, not an exemption. The 2 August 2030 deadline applies to systems intended for public authorities.
- 5. B** The conduit exception covers transient transmission only. Storage, even of encrypted data, is maintaining PHI.
- 6. D** 45 CFR § 164.410: without unreasonable delay and no later than 60 days after discovery.
- 7. C** Assets that provide security functions to the CUI environment are Security Protection Assets, assessed for the capability they provide.
- 8. B** An ESP handling only Security Protection Data stays in scope; its services are assessed as Security Protection Assets.

How Compliance Colleague made this

- Each module started as a question asked in Compliance Colleague, exactly as quoted on the module page. The product answered from the text of the standard and cited the clause or article behind each point.
- Those answers are published in full in the answer archive at compliancecolleague.ai/answers. These notes rewrite them as teaching points; no new facts were added.
- Every teaching point and quiz answer was checked against the archive answer it comes from before publication.

Drafted with AI (Compliance Colleague) from the published answers. Published by Edward Casteloes CISSP, CISA. Compliance Colleague checks an information security policy, a procedure or a network diagram against PCI DSS, the EU AI Act, ISO 42001 and 30+ more, with the clause cited behind every finding. Free trial, no card: compliancecolleague.ai/?ref=cpe



RECORD OF COMPLETION • SELF-STUDY

Four scoping questions practitioners get wrong

Ask the Standard self-study notes, Q4 2026 • About 1 hour • PCI DSS, EU AI Act,
HIPAA, CMMC

PARTICIPANT NAME

CERTIFICATION AND MEMBER ID

DATE COMPLETED

QUIZ SCORE (OUT OF 8)

I confirm that I studied these notes and completed the knowledge check myself.

PARTICIPANT SIGNATURE

Provided by Compliance Colleague (compliancecolleague.ai). This record is self-attested. It is not
an accredited course certificate, and acceptance for CPE is decided by your certifying body.