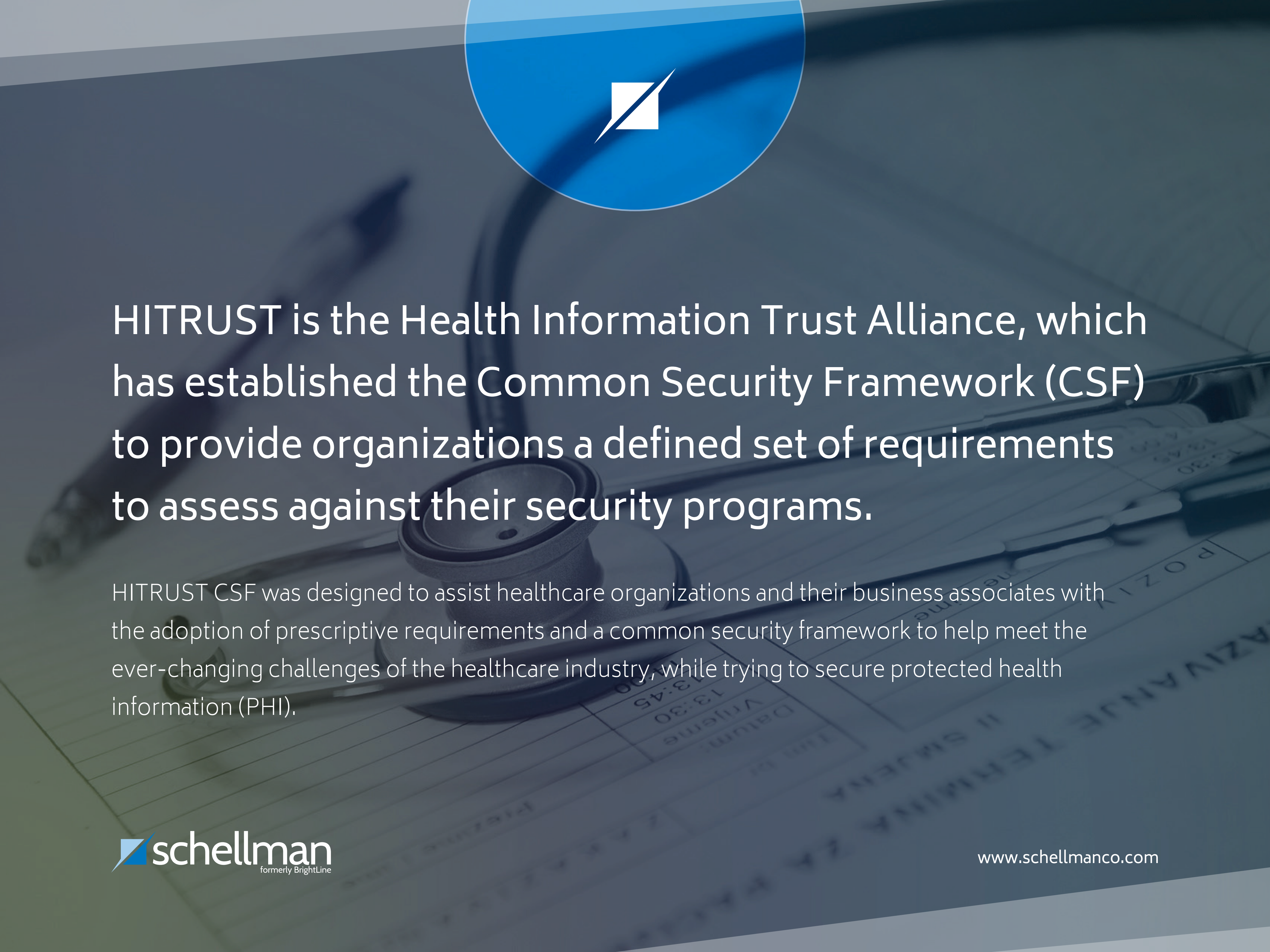
FREQUENTLY ASKED QUESTIONS

THE TOP 15 HITRUST QUESTIONS ANSWERED

schellman
formerly BrightLine

www.schellmanco.com



HITRUST is the Health Information Trust Alliance, which has established the Common Security Framework (CSF) to provide organizations a defined set of requirements to assess against their security programs.

HITRUST CSF was designed to assist healthcare organizations and their business associates with the adoption of prescriptive requirements and a common security framework to help meet the ever-changing challenges of the healthcare industry, while trying to secure protected health information (PHI).

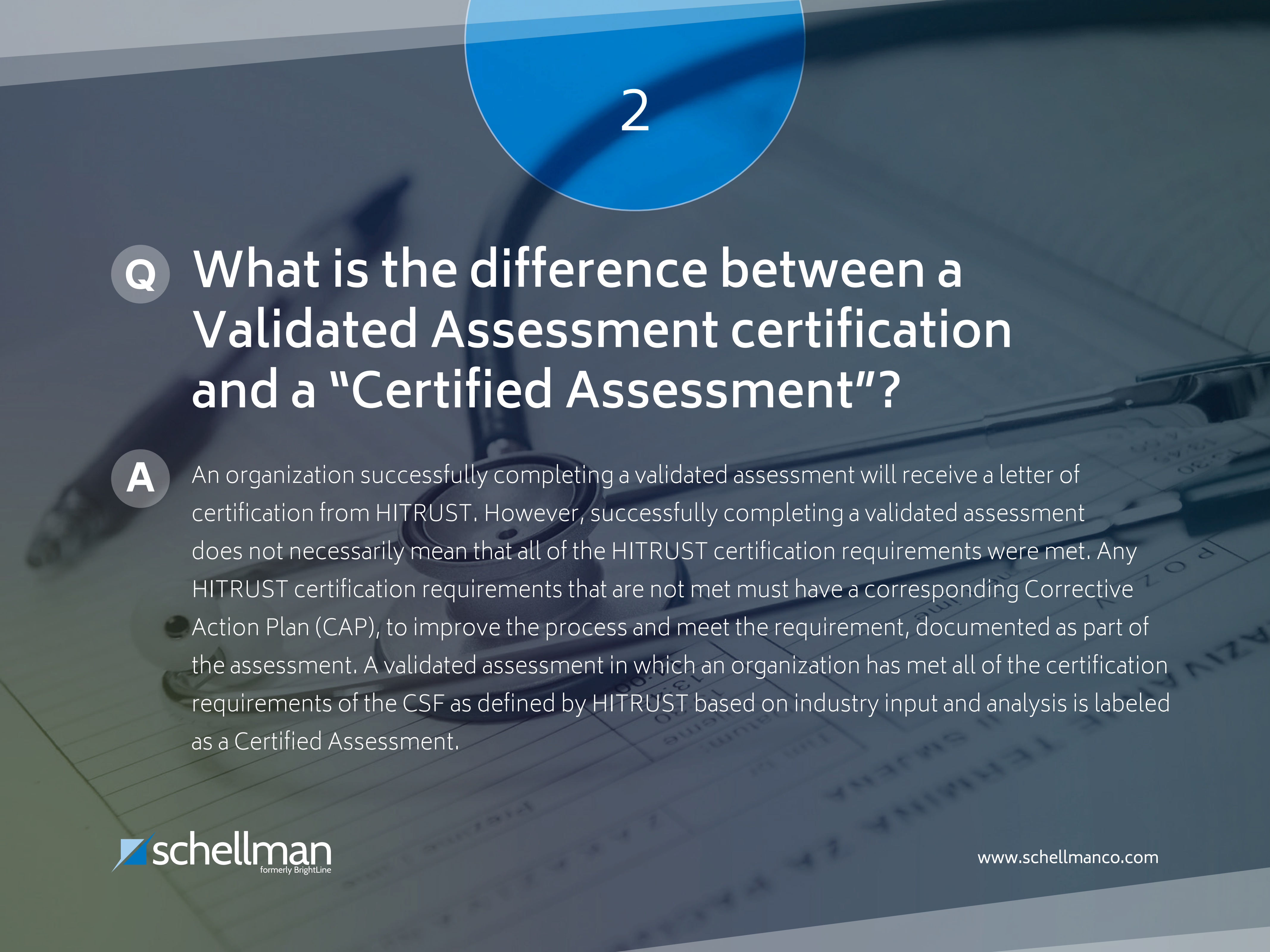
schellman
formerly BrightLine

www.schellmanco.com

1

Q Who issues the certification?

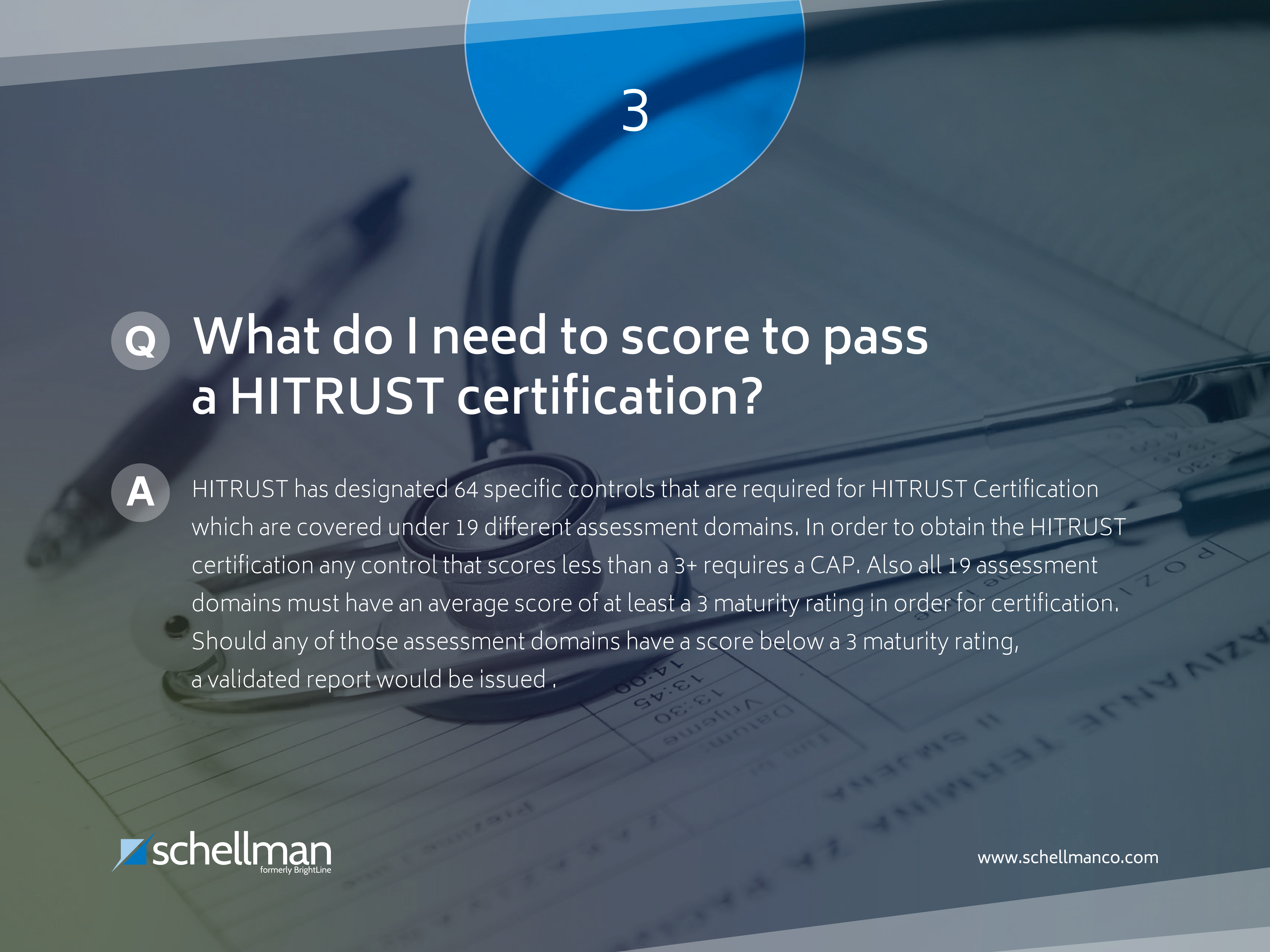
A The CSF Assessor submits their scoring and evidence to HITRUST in the myCSF portal. The results are then reviewed by HITRUST who makes the final determination on scoring and issues the certification if passing scores are obtained in all of the domain areas.



2

Q What is the difference between a Validated Assessment certification and a “Certified Assessment”?

A An organization successfully completing a validated assessment will receive a letter of certification from HITRUST. However, successfully completing a validated assessment does not necessarily mean that all of the HITRUST certification requirements were met. Any HITRUST certification requirements that are not met must have a corresponding Corrective Action Plan (CAP), to improve the process and meet the requirement, documented as part of the assessment. A validated assessment in which an organization has met all of the certification requirements of the CSF as defined by HITRUST based on industry input and analysis is labeled as a Certified Assessment.



3

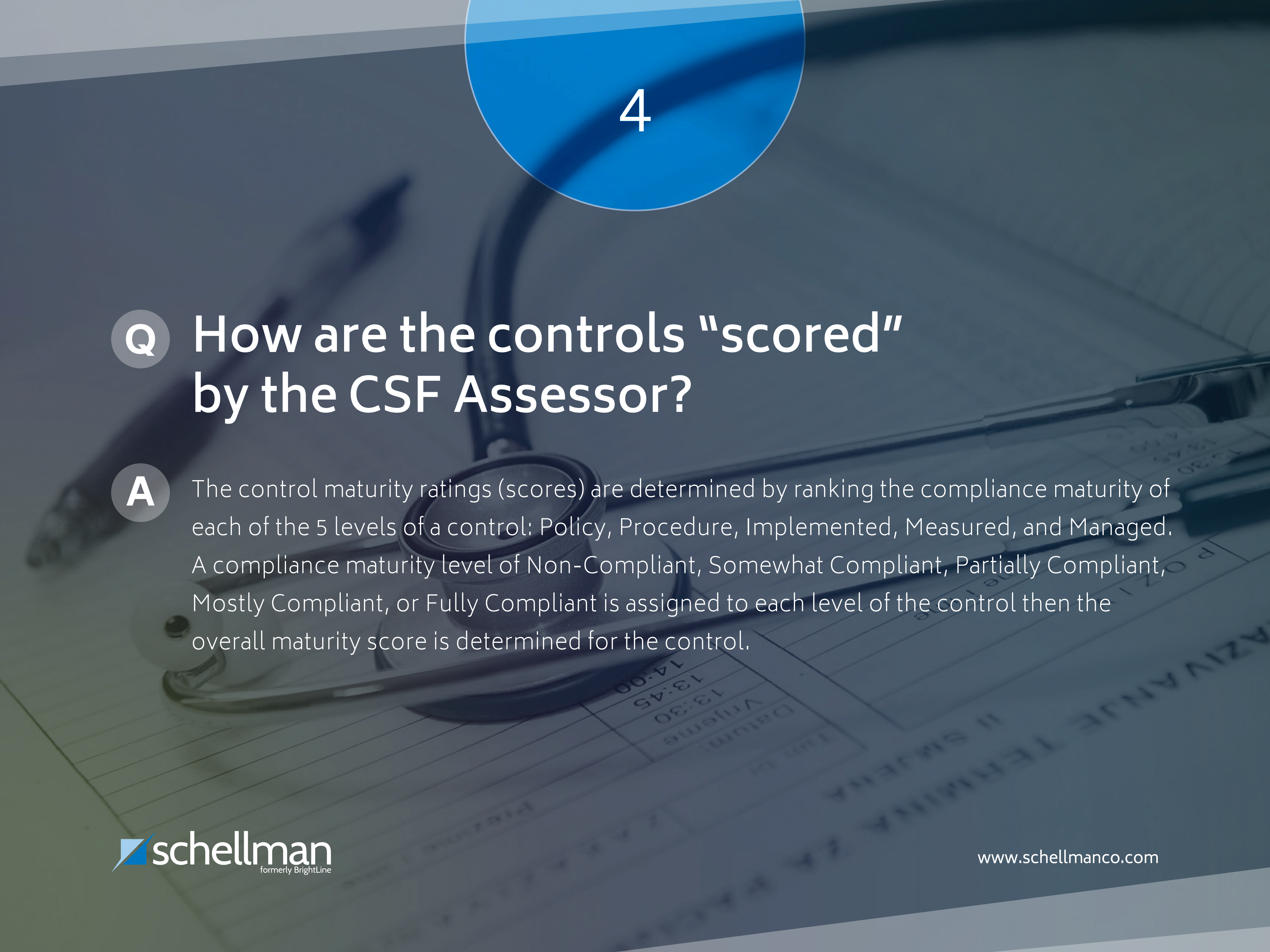
What do I need to score to pass a HITRUST certification?

Q

A

HITRUST has designated 64 specific controls that are required for HITRUST Certification which are covered under 19 different assessment domains. In order to obtain the HITRUST certification any control that scores less than a 3+ requires a CAP. Also all 19 assessment domains must have an average score of at least a 3 maturity rating in order for certification. Should any of those assessment domains have a score below a 3 maturity rating, a validated report would be issued .

schellman
formerly BrightLine



4

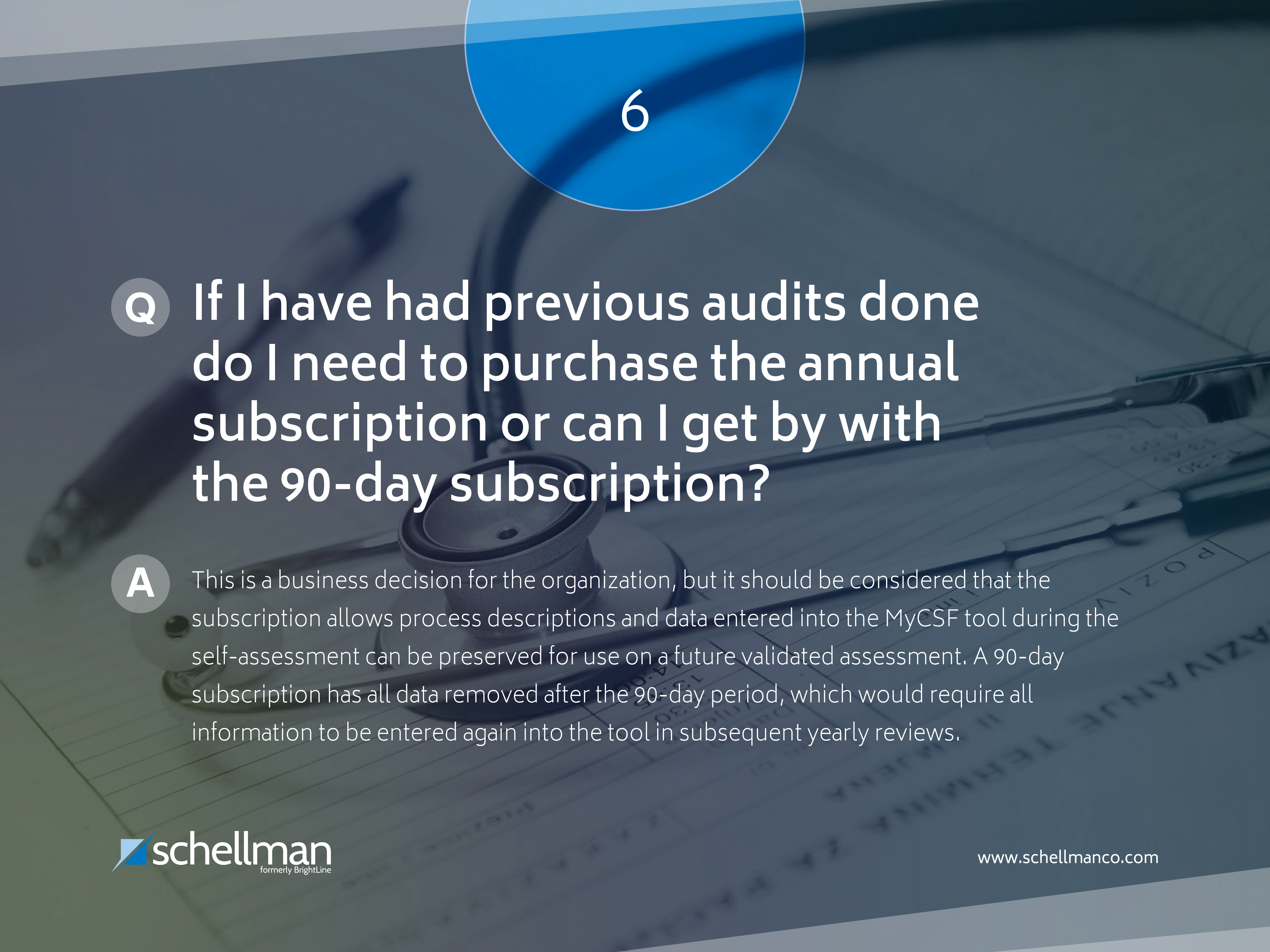
Q How are the controls “scored” by the CSF Assessor?

A The control maturity ratings (scores) are determined by ranking the compliance maturity of each of the 5 levels of a control: Policy, Procedure, Implemented, Measured, and Managed. A compliance maturity level of Non-Compliant, Somewhat Compliant, Partially Compliant, Mostly Compliant, or Fully Compliant is assigned to each level of the control then the overall maturity score is determined for the control.

5

Q Are all organizations HITRUST certified based on the same control implantation requirements?

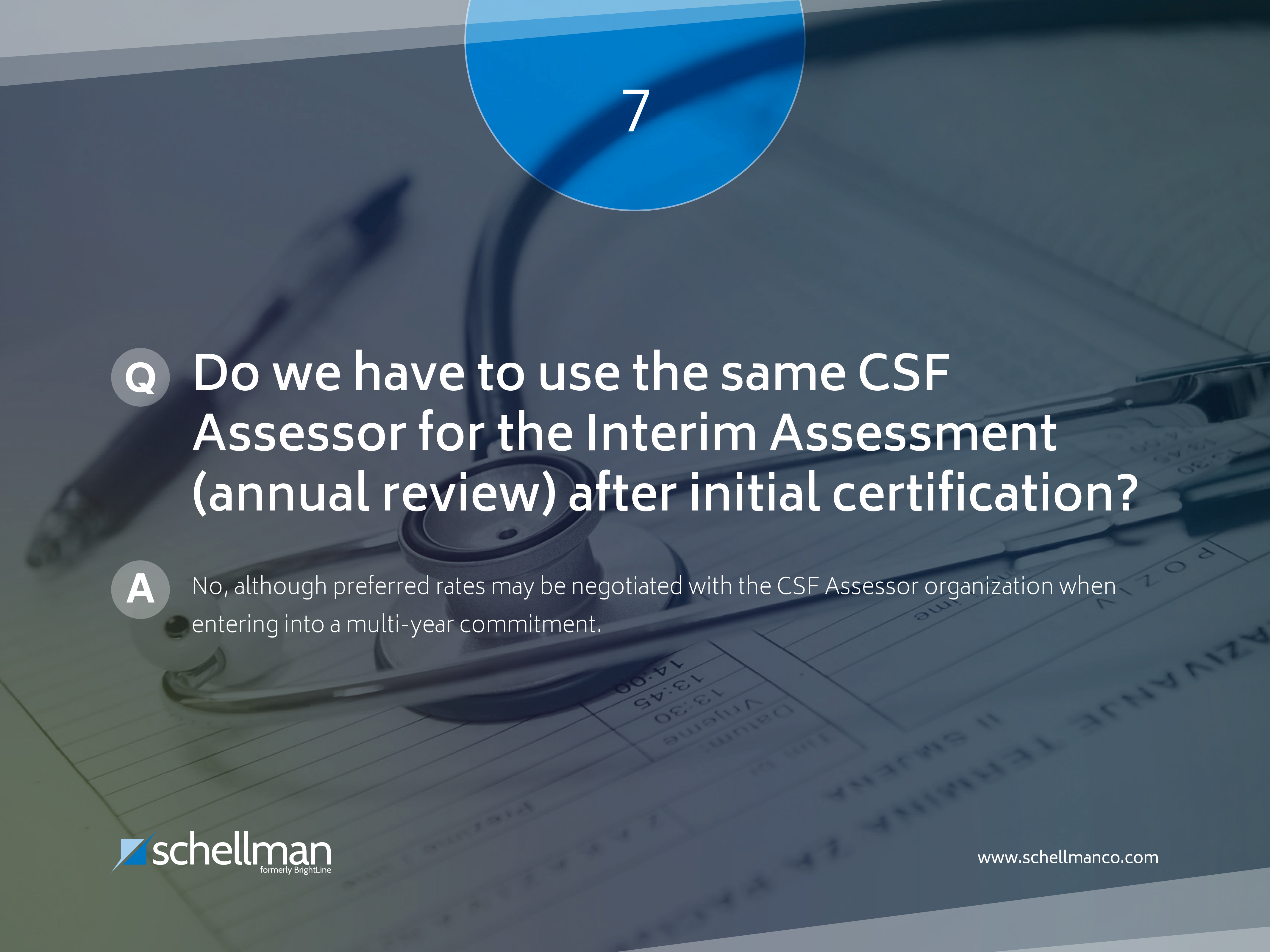
A No, there are 3 levels of implementation requirements (1, 2, and 3). The level of implementation requirement for each individual control is based on an organization's environment and risk as entered in the risk factors tab in the MyCSF tool. Level 1 is the minimum set of security requirements for all systems and organizations regardless of size, sophistication, or complexity. Level 2 or Level 3 would be required only for organizations and systems of increased risk and complexity. A control identified to be Level 3 would need to have requirements in Levels 1 and 2 also implemented.



6

Q If I have had previous audits done do I need to purchase the annual subscription or can I get by with the 90-day subscription?

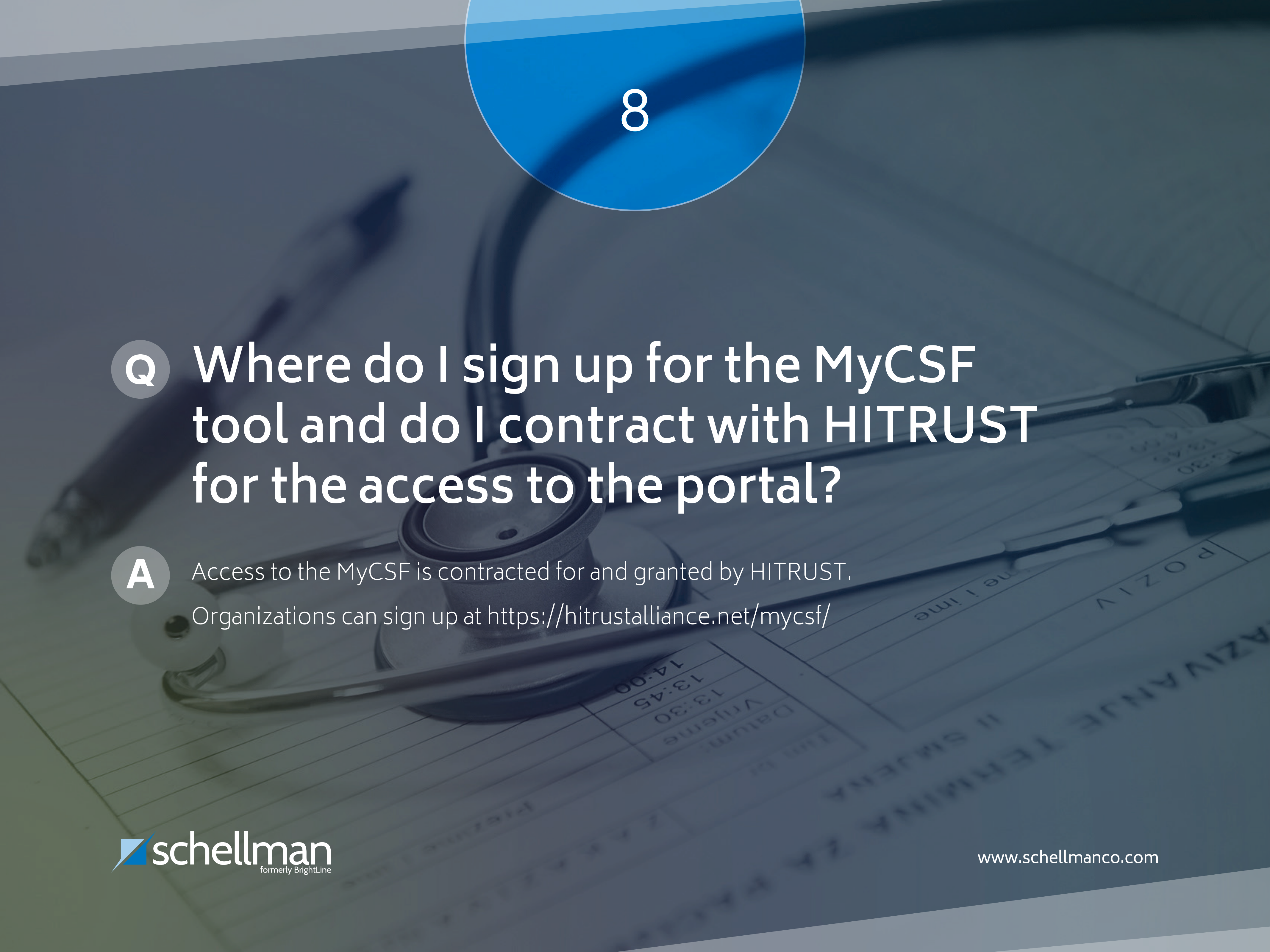
A This is a business decision for the organization, but it should be considered that the subscription allows process descriptions and data entered into the MyCSF tool during the self-assessment can be preserved for use on a future validated assessment. A 90-day subscription has all data removed after the 90-day period, which would require all information to be entered again into the tool in subsequent yearly reviews.



7

Q Do we have to use the same CSF Assessor for the Interim Assessment (annual review) after initial certification?

A No, although preferred rates may be negotiated with the CSF Assessor organization when entering into a multi-year commitment.



8

Q Where do I sign up for the MyCSF tool and do I contract with HITRUST for the access to the portal?

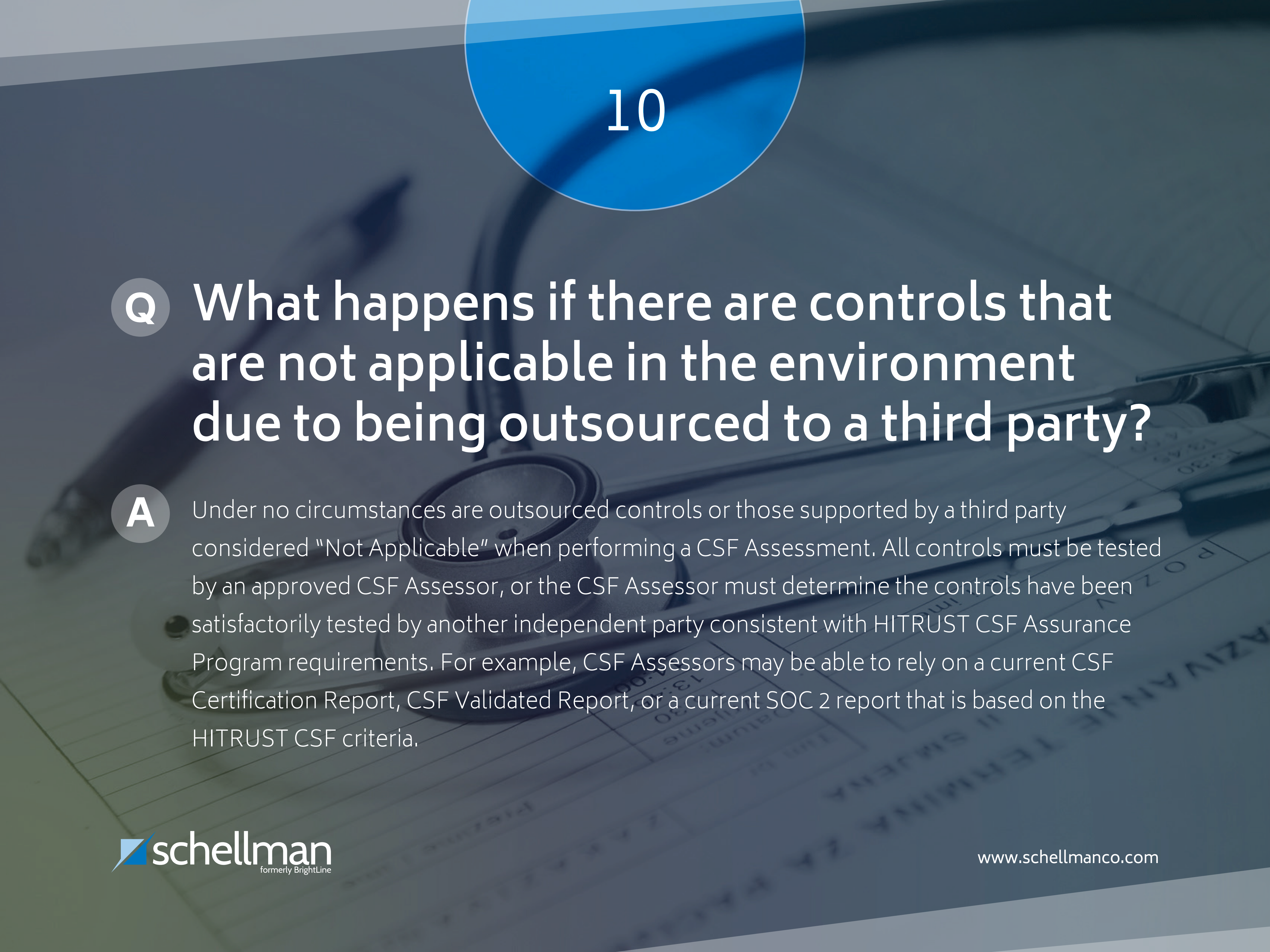
A Access to the MyCSF is contracted for and granted by HITRUST.

Organizations can sign up at https://hitrustalliance.net/mycsf/

9

Q Is the self-assessment a certification?

A No, however the HITRUST-reviewed self-assessment report can be externally distributed to evidence the organization's progress toward a HITRUST certification.



10

Q What happens if there are controls that are not applicable in the environment due to being outsourced to a third party?

A Under no circumstances are outsourced controls or those supported by a third party considered "Not Applicable" when performing a CSF Assessment. All controls must be tested by an approved CSF Assessor, or the CSF Assessor must determine the controls have been satisfactorily tested by another independent party consistent with HITRUST CSF Assurance Program requirements. For example, CSF Assessors may be able to rely on a current CSF Certification Report, CSF Validated Report, or a current SOC 2 report that is based on the HITRUST CSF criteria.

11

Q If I have multiple platforms with different processes that house ePHI, do I need multiple certifications?

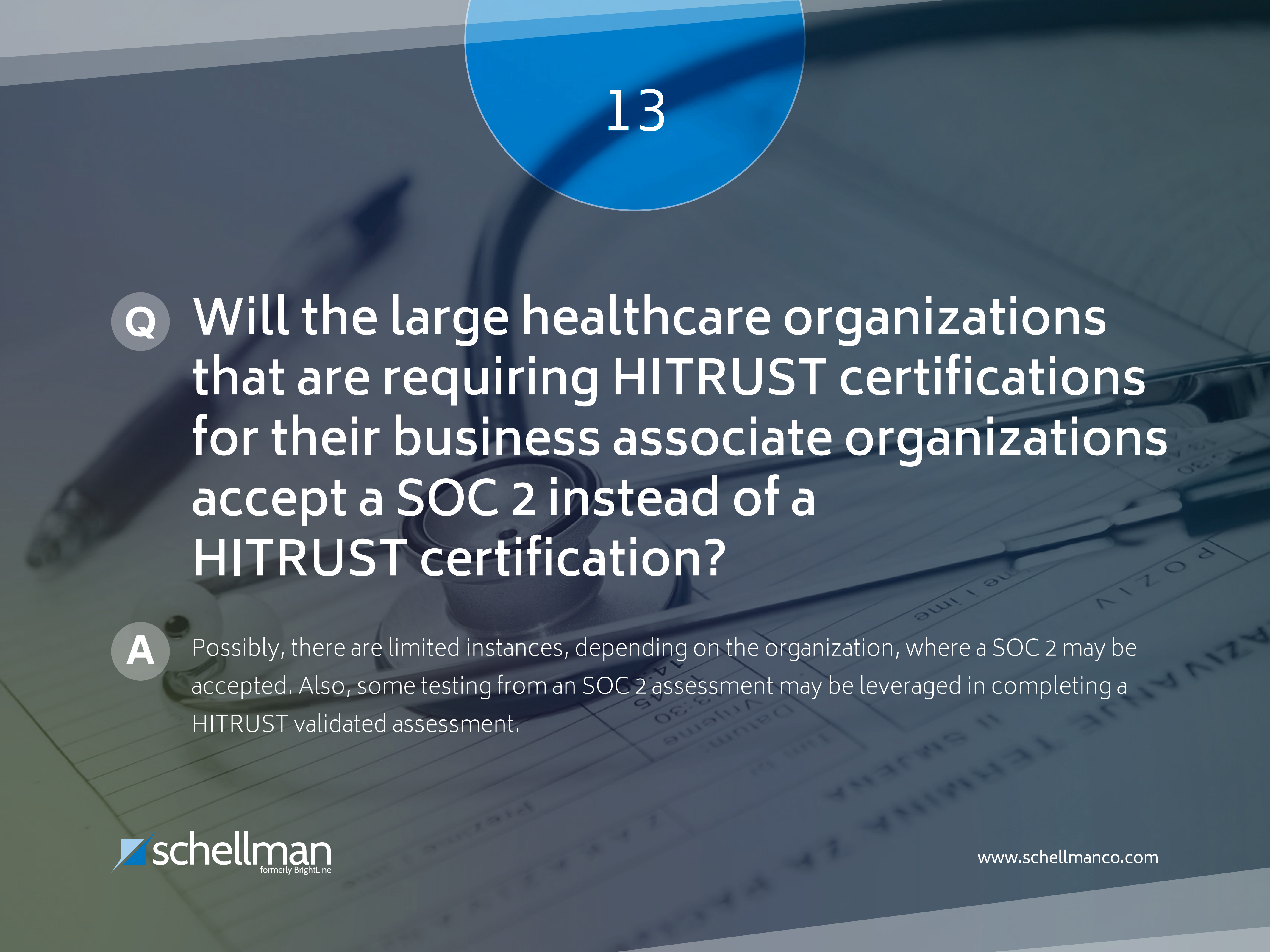
A No. Scope can be determined by the organization, although separate in-scope processes must each be reviewed and documented during the assessment.

12

Q What are the required sampling approaches and methodology?

A HITRUST reviews are required to follow defined sampling methodology based on the frequency of occurrence:

NATURE OF CONTROL AND FREQUENCY OF PERFORMANCE	MINIMUM NUMBER OF ITEMS TO TEST
Manual control, performed daily or many times a day, population › 250	25
Manual control, performed weekly	5
Manual control, performed monthly	2
Manual control, performed quarterly	2
IT General Controls (ITGCs)	Same as guidance for manual controls above
Application Control	Can perform a test of one (test the application contorl once) where ITGCs are tested and determined to be effective; else test the application control 25 times
50-250 items in population	10%
‹50 and not weekly, monthly or quarterly	Use judgment, but consider selecting (5) items or test entire



13

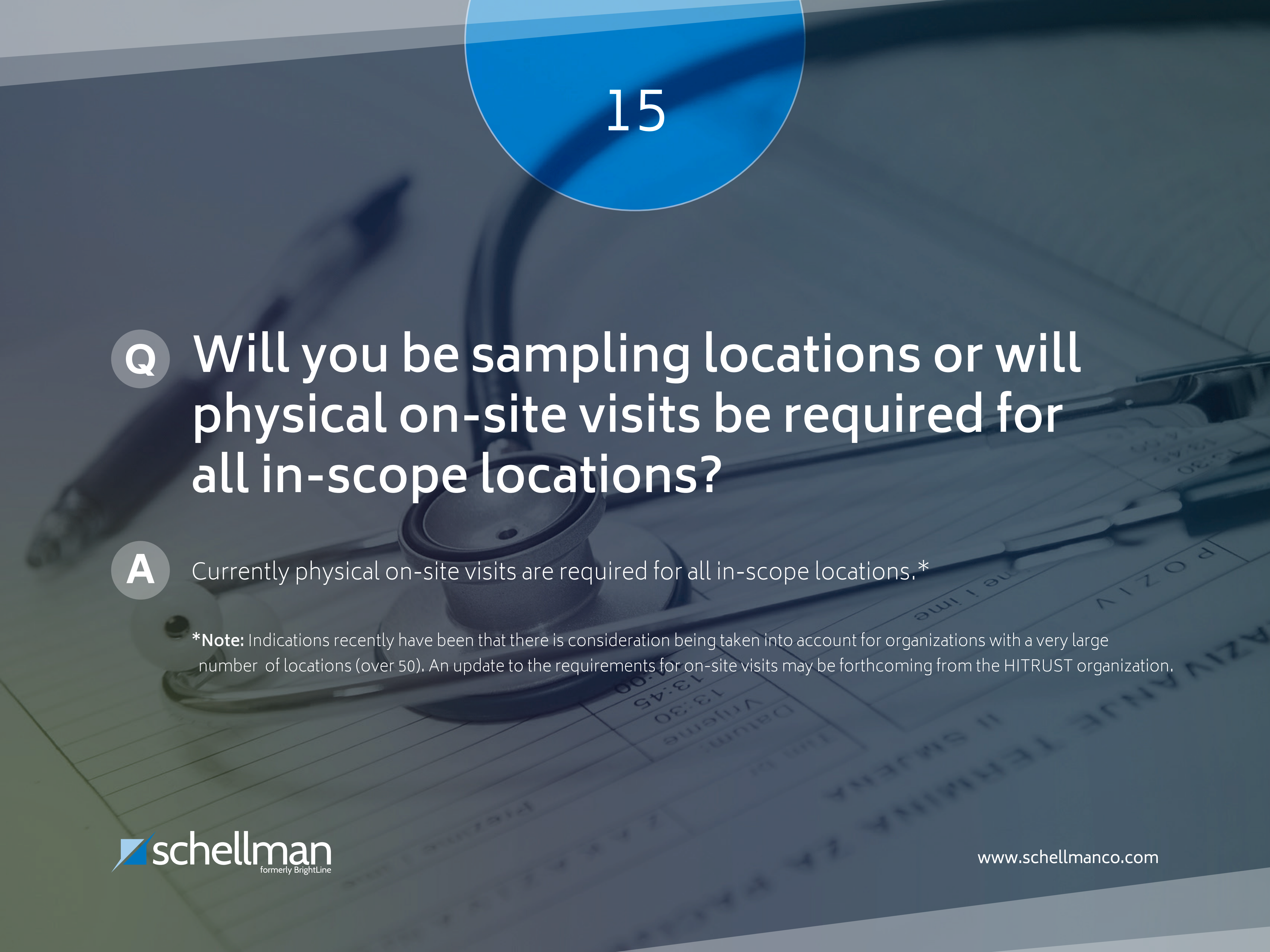
Q Will the large healthcare organizations that are requiring HITRUST certifications for their business associate organizations accept a SOC 2 instead of a HITRUST certification?

A Possibly, there are limited instances, depending on the organization, where a SOC 2 may be accepted. Also, some testing from an SOC 2 assessment may be leveraged in completing a HITRUST validated assessment.

14

Q What if I have environment or process changes during my certification?

A During the annual review process, the responses to the baseline requirements statements in the MyCSF tool must be reviewed and updated to reflect any changes in controls or control requirements since the organization performed its validated assessment. Environment or process changes made after the annual review process are to be documented during a subsequent HITRUST validated assessment.



15

Q Will you be sampling locations or will physical on-site visits be required for all in-scope locations?

A Currently physical on-site visits are required for all in-scope locations.*

***Note:** Indications recently have been that there is consideration being taken into account for organizations with a very large number of locations (over 50). An update to the requirements for on-site visits may be forthcoming from the HITRUST organization.

Discover how Schellman Advantage can help you.

TALK WITH A SPECIALIST

Our Schellman teams have experience performing thousands of attestation examinations. **We're here to answer any questions.**

schellman
formerly BrightLine

www.schellmanco.com

4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
1.866.254.0000

Outside of the United States,
please dial: **+1.973.854.4684**