Frequently Asked Questions (FAQs) for Qualified Security Assessor (QSA) Requirement for Industry-Recognized Professional Certifications

August 2017

A QSA Company is a data security firm certified by the PCI SSC to perform PCI Assessments for clients to ensure that robust policies and procedures are in place to protect cardholder data. QSA employees are individuals who are employed by a QSA Company and have satisfied and continue to satisfy all QSA Requirements.

In 2019 the PCI SSC will increase the industry-recognized professional certifications requirement for QSAs from one industry certification to a minimum of two: one information security and one IT audit certification.

The change is part of the initiative announced in March 2017 to evolve the QSA Program to attract new cyber talent globally and ensure its sustainability and quality in a changing payment environment.

Q 1 What is the change being made to the QSA requirement for industry-recognized professional certifications?

A *The current QSA Qualification Requirements stipulate that QSA employees must hold either an information security certification or an audit certification. The PCI SSC is increasing this requirement to stipulate that QSA employees must have a minimum of two industry certifications: one information security and one IT audit certification.*

The new industry certifications requirement will be effective 1 January 2019 for new QSA employees. For QSA employees qualified and added to the PCI SSC website prior to 1 January 2019, this requirement will be effective 1 July 2019 (for example, upon annual requalification after 30 June 2019).

Q 2 Why is the PCI SSC changing this requirement?

A *This change comes as part of the PCI SSC initiative announced in March 2017 focused on evolving the PCI QSA Program to attract new cyber talent globally and ensure its sustainability and quality in a changing payment environment.*

Q 3 What qualifies as an information security certification?

A *Information security certifications must come from this list:*

List A – Information Security

- *(ISC)2 Certified Information System Security Professional (CISSP)*
- *ISACA Certified Information Security Manager (CISM)*
- *Certified ISO 27001 Lead Implementer*

Q 4 What qualifies as an IT audit certification?

A *IT audit certifications must come from this list:*

List B – Audit

- *ISACA Certified Information Systems Auditor (CISA)*
- *GIAC Systems and Network Auditor (GSNA)*
- *Certified ISO 27001, Lead Auditor, Internal Auditor*
- *IRCA ISMS Auditor or higher (e.g., Auditor/Lead Auditor, Principal Auditor)*
- *IIA Certified Internal Auditor (CIA)*

Q 5 When is this change effective?

A *The new industry certifications requirement will be effective 1 January 2019 for new QSA employees. For QSA employees qualified and added to the PCI SSC website prior to 1 January 2019, this requirement will be effective 1 July 2019 (for example, upon annual requalification after 30 June 2019).*

While QSAs have until 2019 to achieve a minimum of two industry certifications, the PCI SSC encourages QSA Companies not to delay in ensuring their QSA employees will be able to meet this updated qualification requirement.

Q 6 How long do existing QSA employees have to obtain this second industry certification?

A *For QSA employees qualified and added to the PCI SSC website prior to 1 January 2019, this requirement will be effective 1 July 2019 (for example, upon annual requalification after 30 June 2019).*

Q 7 Why is this change being introduced now?

A *The PCI SSC is announcing the change now in order to provide companies and individuals with time to adapt to the change. The QSA Qualification Requirements document is being updated to reflect this change and will be available by the end of 2017.*

Q 8 Is this change being made in response to QSA quality issues?

A *This is not a change in response to specific QSA quality issues. It is part of the PCI SSC's continued focus on ensuring high quality and consistent QSA services for merchants.*

Q 9 When will the updated QSA Qualification Requirements be available?

A *The PCI SSC is in the process of updating the QSA Qualification Requirements document to include this update and plans to publish it by the end of 2017.*

Q 10 How do QSA employees alert the PCI SSC once they have achieved the second industry certification?

A *Once a QSA employee has earned the additional industry certification, they should log into the PCI portal and enter the required information into their consolidated statement page.*

Q 11 Are Associate QSAs required to have industry certifications?

A *Qualification Requirements for Associate QSAs will not include industry certifications.*