Request for Comments (RFC) Process for PCI Security Standards

The Request for Comments (RFC) process described here is an avenue for PCI Security Standards Council (PCI SSC) stakeholders to provide feedback on existing and new PCI Security Standards. This feedback plays a critical role in the ongoing maintenance and development of such resources for the payment card industry. PCI SSC developed this summary and the *RFC Process Guide*, available on the PCI SSC website, to help stakeholders understand and participate in the RFC process.

Depending on the RFC topic, stakeholders may include subject matter experts (SME), Participating Organizations (PO), applicable assessors, Approved Scanning Vendors (ASV), the PCI SSC Board of Advisors, PCI-Recognized Labs, PCI vendors, task force members, and others.

REVISION TYPES

Major – Significant updates to address technology changes or current threats to the payment ecosystem; may require investment by complying entities.

Minor – Additions or modifications that change the intent of sub-requirements and/or testing procedures.

Limited – Changes to sub-requirements and/or testing procedures to clarify intent or address confusing language.

Errata – Clerical corrections, format updates, or updates to amend future-dated requirements that have become mandatory. Errata-only versions are not subject to RFC.

How the RFC Process Enables Collaboration

The RFC Process is for all PCI Security Standards—both new standards under development and existing standards subject to revision. It establishes clear points of collaboration for stakeholder feedback and describes how the feedback is actioned once received.

Multi-purpose – RFCs are used for three types of revisions (see sidebar). The depth of an RFC depends on the type of revision required.

Flexible – Depending on the topic and revision type, an RFC requesting feedback on an initial draft or on proposed modifications may first be directed to certain SMEs, after which it is made available to the full body of affected stakeholders. In other cases, the initial RFC is made directly available to all affected stakeholders.

Comprehensive – All new standards and major revisions to existing standards undergo a minimum of two RFCs. Minor revisions have at least one RFC.

Scheduled – All RFCs are open for a minimum of 30 days. Stakeholders will be notified in advance as to when they can participate in a given RFC.

Feedback – When there is more than one RFC period for a document, a feedback summary document (with all feedback comments and actions) is included for review with the next respective RFC. In all cases, a feedback summary document is made available for stakeholders after the standard is published.

July 2021

PCI Security Standards Council

PCI SCC Request for Comments Process

Provide Community Notice
At least 14 days prior to a new RFC, via targeted e-mails.

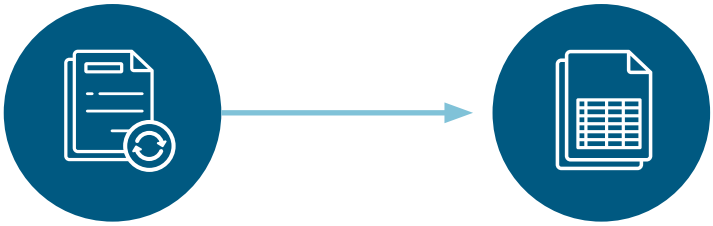
Prepare Documents for RFC
Subject documents may include the standard, summary of changes, supporting documents.

Prepare Portal for RFC
A secure online tool with a unique page for each RFC, to review documents and organize feedback.

Open RFC
Stakeholders sign NDA, review documents, and submit comments, receiving e-mail reminders throughout RFC period.

Close RFC
PCI SSC will not accept feedback after the RFC is closed.

PCI SSC Reviews Feedback and Records Action Taken
PCI SSC reviews feedback and records actions taken including: addressed, future consideration, acknowledged, not adopted.



Finalize Documents
Subject documents are updated to address feedback received.

Post Feedback Summary for RFC Participants
Includes each feedback item received, the company that provided the feedback, and how PCI SSC actioned each feedback item.

July 2021

PCI Security Standards Council