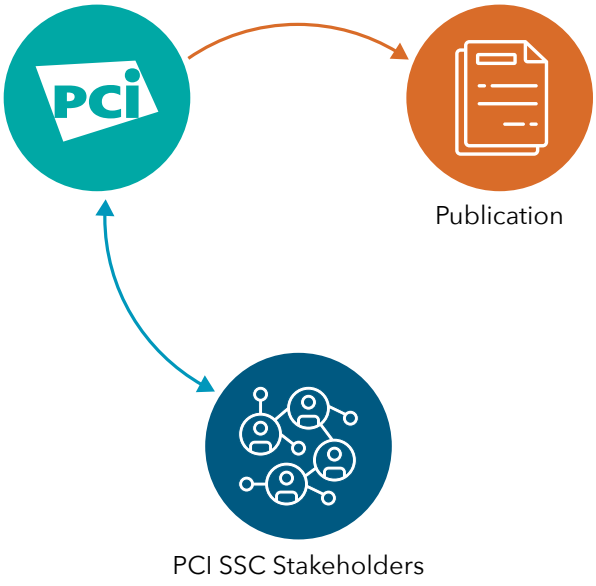
Request for Comments (RFC) Process for PCI Security Standards

The Request for Comments (RFC) process described in this At-a-Glance 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 these 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 RFC topic, stakeholders may include Subject Matter Experts (SME), Participating Organizations (PO), applicable assessors, Approved Scanning Vendors (ASV), the PCI SCC Board of Advisors, PCI 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 – new or modified sub-requirements or testing procedures, minor deadline changes, or updates addressing new threats

Limited – such as amending future-dated requirements that have become mandatory

Errata – clerical corrections or updates; 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 topic and revision type, an RFC may initially be targeted to Subject Matter Experts requesting feedback on an initial draft or proposed modifications, after which it is made available to the full body of affected stakeholders. In some cases, the initial RFC is made directly available to all affected stakeholders.

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

Scheduled – The duration of all RFCs is 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.

February 2019

PCI Security Standards Council

PCI SCC Request for Comments Process

Public Notice Provided
At least 14 days prior to a new RFC via targeted emails

RFC Prepared
PCI Council determines purpose, questions, format, categories, etc.

Documents for RFC Prepared
Includes Standard, Summary of Changes, Supporting Documents

RFC Portal Prepared
Unique page for each RFC, secure online tool for reviewing documents and organizing feedback

RFC Opened
Stakeholders sign NDA, review documents, submit comments; stakeholders receive email reminders during RFC period

RFC Closed, Feedback Reviewed
PCI Council reviews and categorizes all feedback items

Record Final Action Taken
Such as requirement added, evolved or clarified; guidance added or clarified; no action

Standard Documents Finalized
Subject documents are updated to address feedback received

Feedback Summary Posted
Includes each feedback item received, which company provided that feedback, and how the PCI Council actioned each feedback item

February 2019

PCI Security Standards Council ®