

# Request for Comments (RFC) Process Guide

VERSION 1.0 | FEBRUARY 2019



## Purpose of this Guide

Request for comment (RFC) periods are avenues for 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 *RFC Process Guide* to help stakeholders understand and participate in the RFC process.

## Applicable Documents and Details

**Table 1: PCI SSC RFCs: Applicable Documents and Details**

PCI SSC Document (See Table 2 - Revision Types for PCI SSC Standards)	Purpose of RFC <sup>[1]</sup>	RFC Audience <sup>[2]</sup>	Minimum Number of RFCs	Minimum Duration of RFC <sup>[3]</sup>	When RFC Feedback is Provided to POs <sup>[4]</sup>
New Standard (not previously released)	Feedback on an initial draft	SME <sup>[5]</sup>	Two	30 days	With next RFC
	Feedback on updated draft, including proposed modifications from first RFC	Full		30 days	After standard is published
Existing standard – major revision (e.g., v1.0)	Feedback on current version <sup>[6]</sup>	Full or SME <sup>[5]</sup>	Two	30 days	With next RFC
	Feedback on updated draft, including proposed modifications from first RFC	Full			After standard is published
Existing standard – minor revision (e.g., v1.1)	Feedback on proposed modifications to current version	Full	One	30 days	After standard is published
Existing standard – limited revision (e.g., v1.1.1)	Feedback on proposed modifications to current version	SME <sup>[5]</sup>	One	30 days	After standard is published

<sup>[1]</sup> PCI SSC may conduct RFCs on either a complete or a partial standard, as needed.

<sup>[2]</sup> Audience determined by RFC topic, but typically includes POs, applicable assessors, ASVs, the PCI SSC Board of Advisors, PCI labs, PCI vendors, taskforce members, and others.

<sup>[3]</sup> Calendar days.

<sup>[4]</sup> PCI SSC will post RFC feedback in the PCI SSC portal.

<sup>[5]</sup> Subject Matter Experts (SME) – Depending on the standard, different SME audiences may be asked to participate in a targeted RFC. For example, a task force, the PCI SSC Board of Advisors, or PTS labs may be asked to review updates to specific documents pertinent to their roles with PCI SSC.

<sup>[6]</sup> May be a clean current version or include proposed changes.

**Note:** Other PCI SSC documents may be provided for a formal RFC period under the Exception Process outlined in Table 4 of this document. Any other deviations to RFC processes documented herein are also subject to the Exception Process below.

## Revision Types

**Table 2: Revision Types for PCI SSC Standards**

Type of Revision	Potential Reasons for Revision
<b>Major</b> (e.g., v1.0)	<ul style="list-style-type: none"> <li>• Restructure of standard such that reporting structure, portals, etc. need to change.</li> <li>• Significant updates to address technology changes or current threats to the payment ecosystem; may require investment by complying entities.</li> </ul>
<b>Minor</b> (e.g., v1.1)	<ul style="list-style-type: none"> <li>• Changes that don't meet threshold of a major revision.</li> <li>• Addition or modification of sub-requirements and/or testing procedures.</li> <li>• Changes that result in an update to implementation deadlines.</li> <li>• Examples include updates to address a new vulnerability or threat.</li> </ul>
<b>Limited</b> (e.g., v1.1.1)	<ul style="list-style-type: none"> <li>• Changes that do not meet the threshold of minor revision.</li> <li>• Examples include updates to amend future-dated requirements that have become mandatory.</li> </ul>
<b>Errata</b>	<ul style="list-style-type: none"> <li>• Clerical errors such as typographical errors and mis-numbering.</li> <li>• Updates that only consist of errata are not subject to RFC.</li> <li>• Major, minor, or limited revisions that also include errata will be subject to RFC per this <i>PCI SSC RFC Process Guide</i>.</li> </ul>

## RFC Process

**Table 3: PCI SSC RFC Process Steps**

Process Steps	Details
1. PCI SSC provides community with notice prior to start of RFC.	<ul style="list-style-type: none"> <li>• PCI SSC updates public RFC calendar with upcoming RFCs as soon as RFC timing is known.</li> <li>• A minimum of 14 days' notice prior to start of RFC via targeted emails.</li> <li>• Community opts in (via the PCI SSC portal) regarding topic areas for which they want to receive RFC notifications.</li> </ul>
2. PCI SSC prepares the RFC.	<p>Determine purpose, questions, format, categories, etc. For example:</p> <ul style="list-style-type: none"> <li>• Open feedback               <ul style="list-style-type: none"> <li>– General feedback on sections/requirements</li> </ul> </li> <li>• Targeted feedback               <ul style="list-style-type: none"> <li>– Specific questions for participants to answer</li> </ul> </li> <li>• May include options for participants to categorize for their feedback—e.g.:               <ul style="list-style-type: none"> <li>– Request for additional guidance</li> <li>– Request for clarification</li> <li>– Request for new/updated requirement</li> </ul> </li> </ul>
3. PCI SSC prepares documents for the RFC.	<p>Documents included with an RFC can include:</p> <ul style="list-style-type: none"> <li>• Standard</li> <li>• “Read Me First” document with RFC overview and instructions</li> <li>• Summary of Changes document</li> <li>• Other documents related to the standard</li> <li>• Other documents that aid the participants' understanding of the RFC</li> </ul>

Process Steps	Details
4. PCI SSC prepares the PCI SSC portal for the RFC.	<p>Each RFC has its own page to meet specific RFC requirements, including:</p> <ul style="list-style-type: none"> <li>• Confirmation of NDA covering the RFC documents</li> <li>• Specifics of the standard or other document subject to RFC</li> <li>• Type of feedback requested and structure for feedback submission</li> <li>• Any unique information about the RFC or subject document that the RFC audience should be aware of</li> </ul>
5. PCI SSC opens the RFC.	<ul style="list-style-type: none"> <li>• RFC is open for at least the time defined in Table 1 in this <i>PCI SSC RFC Process Guide</i>.</li> <li>• RFC participants utilize the PCI SSC portal to sign the non-disclosure agreement, download the RFC document(s), and submit RFC comments.</li> <li>• RFC participants receive reminder notices via email during RFC period.</li> </ul>
6. PCI SSC closes the RFC and reviews feedback received.	<p>PCI SSC reviews and categorizes all feedback items by type of change requested</p> <p>Example categories:</p> <ul style="list-style-type: none"> <li>• Request for clarification</li> <li>• Request for guidance</li> <li>• Evolving requirement (add, change, or delete a requirement to reflect changing technology)</li> <li>• Update program (for a PCI SSC program rather than a standard or document)</li> <li>• Feedback unrelated to purpose of RFC (e.g., for another standard)</li> <li>• Editorial/typo/format fix</li> <li>• Compliance comment intended for the payment brands</li> <li>• No change requested</li> </ul> <p>As appropriate, PCI SSC may follow up with feedback provider if intent of feedback is unclear.</p>
7. PCI SSC records the final action taken for all feedback items.	<p>Example actions taken:</p> <ul style="list-style-type: none"> <li>• Requirement added, evolved, or clarified</li> <li>• Guidance added or clarified</li> <li>• Addressed in supporting document (e.g., in Program Guide, Reporting Template, etc.)</li> <li>• Retained for later consideration</li> <li>• No action (e.g., no change was requested, feedback was unclear, feedback suggestion does not align with intent of standard or is considered out of scope for this program or for PCI SSC)</li> </ul>

Process Steps	Details
8. PCI SSC finalizes document updates.	Subject document is updated to address feedback received.
9. PCI SSC prepares and posts the RFC feedback summary document.	<p>The feedback summary document will include at least the following information:</p> <ul style="list-style-type: none"> <li>• Summary of feedback categories received (e.g., via charts or graphs)</li> <li>• Explanations of PCI SSC actions taken (e.g., more details about each type of action)</li> <li>• List of companies that provided feedback</li> <li>• A full summary of all feedback provided, including: <ul style="list-style-type: none"> <li>– Company that provided the feedback</li> <li>– Company profile (e.g., merchant, vendor, financial institution)</li> <li>– Related sections of subject PCI SSC document</li> <li>– Actual feedback received, including comments and suggested solutions</li> </ul> </li> </ul> <p><b>Note:</b> PCI SSC will redact feedback if deemed appropriate to avoid propagation of security flaws or risks, or to protect proprietary information or privacy.</p> <ul style="list-style-type: none"> <li>– PCI SSC feedback category</li> <li>– PCI SSC actions taken for each item</li> </ul>

## Exceptions to PCI SSC RFC Process

This exception process will be followed whenever a PCI SSC Working Group or Committee determines it is necessary to deviate from the *PCI SSC RFC Process Guide*. Examples of exceptions may include:

- Submitting a document for RFC that is not included in Table 1 of this document.
- Submitting an RFC to a different audience than defined in Table 1 of this document.
- Submitting a different number of RFCs than defined in Table 1 of this document.
- Setting an RFC duration that is less than the minimum defined in Table 1 of this document.
- Providing notice before starting an RFC that is less than the minimum notice defined in Table 3 of this document.

**Table 4: PCI SSC RFC Exception Process**

Process Step	Details
PCI SSC working group or other PCI SSC committee determines it is necessary to vary from this <i>PCI SSC RFC Process Guide</i> .	<ul style="list-style-type: none"> <li>• Working group/committee prepares Issue Summary, outlining details and justification for proposed variance.</li> <li>• Approval is required by the PCI SSC Management Committee, with notice sent to the Executive Committee.</li> </ul>