

# Read Me First: Instructions and Guidance for PCI DSS v4.0.1 Draft for RFC



# Thank you in Advance!

- First and foremost, the PCI SSC would like to thank you for taking the time to review PCI DSS v4.0.1 Draft for RFC.
- Your thorough review is welcome and is fundamental to our revision process. The following slides will guide your review.

## And Please...

- Read this RFC guidance in its entirety before beginning your review.
- Plan your reviews ahead of time and ensure your feedback is submitted before the RFC period closes.

# PCI DSS v4.0.1 Draft – RFC Overview



- The RFC period will run from 13 December through 24 January
- Be sure to submit all feedback by 8:00pm Eastern Time on 24 January
  - Note: Late feedback will not be accepted
- Your feedback, your organization's name, and how PCI SSC actioned your feedback will be made available for review by RFC participants
  - Review the PCI SSC [RFC Process Guide](#) for more information
  - Please avoid including company sensitive information and remember to keep your comments professional and collaborative

# Accessing the Documents

- *Only your company's primary contact may log into the portal and download the RFC documents.*
  - If you do not know who your company's primary contact is, please send an email to [RFC@pcisecuritystandards.org](mailto:RFC@pcisecuritystandards.org) for assistance.
- Log-in to the portal: <https://programs.pcissc.org> with your username and password.
  - If you don't know your password, click "Forgot your password" to create a new password.
  - If you do not have a username, please contact [RFC@pcisecuritystandards.org](mailto:RFC@pcisecuritystandards.org) for assistance.
- Click on "PCI DSS v4.0.1 DRAFT for RFC."
- Accept the Group Participation Agreement (the NDA) to download the documents.
- Click to download each of the following documents for this RFC:
  - PCI DSS v4.0.1 Draft for RFC
  - Summary of Changes from PCI DSS v4.0 to PCI DSS v4.0.1

# Submitting Feedback

- To enter feedback:
  1. *Select the Document, Section, and Category of feedback*
    - *Note: only those PCI DSS sections with substantive updates are included in the drop-down menu in the RFC Portal*
  2. *Enter the sub-section (for example, Requirement X.X.X) to identify the specific area to which your feedback refers*
  3. *Enter the page number*
  4. *Enter your Comments and Suggested Solution for each feedback item.*
- Ensure your work is saved - after each entry and before you exit the portal, select “Save Draft Comments.”
  - You can come back later to finish entering feedback; you do not need enter all feedback in the same session.
- When all your feedback is complete, select “Submit Feedback” and then select “Ok” to confirm your submission is complete.
  - Once you select “Ok,” you will be unable to edit your feedback.
  - A confirmation email will be sent after you submit your feedback.
- Alternatively, you can download the feedback spreadsheet, input your feedback, save, and then upload the spreadsheet back to the Portal.

# To maximize the value of your feedback:

- In the Comment field, explain the reason for your feedback.
  - For example, describe why a statement is unclear.
- In the Suggested Solution field, include a recommendation to address your comments.
  - For example, suggest new language to add clarity or ask for specific additional guidance.
- Be as detailed as possible with your comments and suggested solutions.
- Feel free to leave either the Comment or Suggested Solution fields blank.
  - It is not necessary to copy the same information into both fields.
- *Do not submit the same feedback item more than once.*
  - This is unnecessary since PCI SSC reviews every feedback item submitted.
- Consolidate all feedback for your company since you can only provide 50 feedback entries.
- Contact [RFC@pcisecuritystandards.org](mailto:RFC@pcisecuritystandards.org) with any questions.

# Before You Get Started

- A redline version of PCI DSS v4.0.1 Draft for RFC has been provided.
  - **Feedback is being requested only on the proposed changes tracked in this document.**
- The *Summary of Changes from PCI DSS v4.0 to v4.0.1 Draft* is provided to facilitate your review of the standard.
  - This document highlights key proposed changes between v4.0 and v4.0.1.
  - PCI SSC is not requesting feedback on this document.

# Things to Consider While Reviewing PCI DSS v4.0.1 Draft



- The purpose of this limited revision is to:
  - Address feedback and questions PCI SSC has received from stakeholders.
  - Correct errors and typos, and update and clarify requirements and guidance.

***Refer to the RFC Process Guide on the PCI SSC website to understand the different revision types for PCI SSC Standards.***

# FAQ 1

---

## *Are any of these proposed updates going to change how we implement the new requirements?*

- The proposed updates are intended to support organizations as they transition to v4.0 by providing clarifications and additional guidance.
- Depending on an organization's current security controls, some updates may provide additional flexibility for meeting new requirements.

## FAQ 2

---



### *When can we expect this revision to be published?*

As communicated during the 2023 Community Meetings, PCI DSS v4.0.1 is expected for publication in the first half of 2024.

## FAQ 3

---

***Can we expect to see any requirements removed or added because of this RFC?***

The proposed changes are limited to what is included in the draft of PCI DSS v4.0.1.

## FAQ 4

---

### *Where are the PCI DSS v4.0 Appendix E sample templates to support the customized approach?*

- The sample templates to support the customized approach have been removed from PCI DSS v4.0.1
- To enhance usability, the templates are now located in the PCI SSC website's Document Library
  - Filter on "PCI DSS" and search for "Sample Templates: Customized Approach"