PCI Security Standards Council

Standards Development Policy

Version 1.0

January 2023

Document Changes

Date	Version	Description
January 2023	1.0	First release

Table of Contents

1. Introduction[1]

This PCI Security Standards Council ("PCI SSC" or the "Council") Standards Development Policy (the "Policy") describes PCI SSC's policies and procedures for the development, approval and release of PCI SSC Standards and Work Items. Capitalized terms used but not otherwise defined in this Policy have the meanings specified in Section 3 below or in the PCI SSC IPR Policy, as applicable.

1.1 Purpose

This Policy establishes transparent policies and procedures for the development, approval and release of PCI SSC Standards and Work Items. This Policy does not address the specific details relating to development work performed at the Working Group level.

1.2 Overview

The mission undertaken by PCI SSC is to enhance global payment data security by developing standards and supporting services that drive education, awareness, and effective implementation by stakeholders. This mission is undertaken with the understanding that the threat landscape in which our documents and services are developed is constantly evolving. To meet the challenges posed by this changing threat landscape, and to ensure the on-going quality and efficacy of our Standards, PCI SSC looks to our community of stakeholders to assist with the development and validation of our Standards, products, and services.

This policy outlines the process used for the development and release of our Standards documents, and other work items, in a way that embeds stakeholder feedback into all aspects. Merchants, other companies, and even individuals can play a role, by participating in RFCs, Special Interest Groups, and - as members of the Board of Advisors - the Standards approval process itself.

2. Related Publications

Document	Definition / Description
Charter of the Board of Advisors[2]	The then current version of the PCI SSC Charter of the Board of Advisors, as amended and in effect from time to time and posted on the Website. Describes responsibilities, composition, eligibility, elections and other matters relating to the Board of Advisors.
IPR Policy[3]	The then current version of the PCI SSC Intellectual Property Rights Policy, as amended and in effect from time to time and posted on the Website.
PCI Participant Agreement[4]	The then current version of the PCI Participant Agreement, as amended and in effect from time to time and posted on the Website. Describes PCI SSC's standard terms and conditions for PCI Participants when accessing the PCI Participant Portal.
PCI Participant Rights, Obligations and Rules of Participation[5]	The then current version of the PCI Participant Agreement, as amended and in effect from time to time and posted on the Website. Describes the general rights, obligations and rules of participation for PCI Participants.
RFC Process Guide	The then current version of the PCI SSC Request for Comment (RFC) Process Guide, as amended and in effect from time to time and posted on the Website.

3. Terminology

Term	Definition / Source / Document Reference
Advisor	A PCI Participant serving as a member of the Board of Advisors.
Affiliate Member	A PCI SSC Affiliate Member, as described further on the Website.
Board of Advisors	See Section 4.2.
Fee Schedule	The schedule of annual fees payable by PCI Participants to participate in the PCI Participant Program, as amended and in effect from time to time and posted on the Website.
Founding Member	A PCI SSC Founding Member, per PCI SSC's Limited Liability Company Agreement.
Good Standing	Means that the applicable PCI Participant or Affiliate Member: • Has executed and submitted to PCI SSC the current version of the PCI Participant Agreement or Affiliate Participation Agreement, as applicable • Has paid to PCI SSC all applicable PCI Participant Fees or Affiliate Member dues, as applicable, and • Is otherwise in compliance with all applicable PCI Participant, Affiliate Member, and/or Board of Advisors rules, policies and procedures, including corresponding attendance and voting requirements, as applicable.
Major Standards Work Item	A proposed new PCI SSC Standard or Major Revision to an existing PCI SSC Standard.
Member	A Founding Member or Strategic Member of PCI SSC. For purposes of this Policy, "Member" does not include Affiliate Members, PCI Participants, or members of the Board of Advisors.
Major Revision	Changes to Standards that the Council determines will require: • Restructuring with material impact on reporting structures, portals, and similar matters or • Significant updates to address technology changes or current threats to the payment ecosystem
Other Work Item	A Work Item other than a Major Standards Work Item.
PCI Participant	A participant in the PCI Participant Program that has executed the then current version of the PCI Participant Agreement and pays applicable PCI Participant Fees.

[1] *Document to be approved by ExCo as a "Charter" for purposes of the LLC Agreement prior to release.*
[2] *Posted online:* https://www.pcisecuritystandards.org/Charter_for_Board_of_Advisors.pdf
[3] *Posted online:* *https://www.pcisecuritystandards.org/about_us/policies/#ipr*
[4] *Posted online:* *https://www.pcisecuritystandards.org/PCI-SSC-Group-Participation-Agreement.pdf*
[5] *Posted online:* *https://www.pcisecuritystandards.org/get_involved/rights_responsibilities/*

Term	Definition / Source / Document Reference
PCI Participant Fees	The then applicable annual fees payable to PCI SSC to participate in the PCI Participant Program, determined by PCI SSC based on the PCI Participant's "Class" (See Section 4.1 below) and/or size, as from time to time established by PCI SSC and specified in the Fee Schedule.
PCI Participant Portal	The non-public PCI SSC web portals and associated pages, repositories and content that PCI SSC makes accessible to PCI Participants.
PCI Participant Program	The program operated and managed by PCI SSC and described further herein and on the Website, through which merchants, vendors, developers, acquirers, processors, payment issuers and other industry stakeholders, have the opportunity to participate in the Council's strategic and technical initiatives by providing varying levels of input into to the Standards and Standards Program development process.
REB	Regional Engagement Board. See Section 4.3.
RFC	A PCI SSC Request for Comments. See Section 5.3.
SIG	A Special Interest Group, as further described in Section 4.4.
Standards Program	A program operated and managed by PCI SSC supporting a given Standard or associated certification, training, or security assessment.
Strategic Member	A PCI SSC Strategic Member, as described further on the Website.
Task Force	A Task Force, as further described in Section 4.5.
Third Party Assessors	Security companies qualified by the Council to assess the network environment, facilities, products or solutions of parties unrelated to such assessors for compliance against applicable PCI SSC Standards. For the avoidance of doubt, Third Party Assessors do not include Internal Security Assessors or their "Sponsor" companies.
Website	The then-current PCI SSC Website (and its accompanying web pages), which is currently available at www.pcisecuritystandards.org.
Work Item	A PCI SSC Standard, draft PCI SSC Standard, content intended for inclusion in the foregoing, and associated Standards Program materials and guidance documents.
Working Group	A technical working group established by PCI SSC to develop a Standard, Draft Standard, Other Work Item, or associated Standards Program.

4. Roles and Responsibilities

Each of the following plays a significant role in the development of PCI SSC Standards and other Work Items.

4.1 PCI Participants

Participation as a PCI Participant is open to any interested individual or Organization (defined below) that satisfies applicable eligibility criteria, registers on the PCI Participant registration page accessible through the Website, accepts the PCI Participant Agreement, and pays applicable PCI Participant Fees. The term "Organization" is used broadly to mean any legal entity that is not a natural person (for example, a corporation, association, partnership, company, governmental agency, academic entity, or non-profit organization).

PCI SSC has three classes of PCI Participants (each a "Class"), each with varying rights, obligations, and annual fees:

- Principal Participating Organizations (or "Principal POs") (reserved for Organizations)
- Associate Participating Organizations (or "Associate POs") (reserved for Organizations)
- Individual Participants (reserved for natural persons)

All PCI Participants in Good Standing are eligible to participate (in varying ways, depending on their Class) in a range of PCI SSC activities, including the process for developing PCI SSC Standards and certain Other Work Items. PCI Participants may provide input and receive feedback on Standards and related matters, through participation on the Board of Advisors, and in the RFCs, SIGs, Task Forces, and REBs for which they are eligible. Participation is subject to the terms of the PCI Participant Agreement and the PCI Participant Rights, Obligations and Rules of Participation, and all comments, suggestions, feedback, and other input provided by PCI Participants are subject to the intellectual property rights provisions of the PCI Participant Agreement and IPR Policy.

4.2 Board of Advisors

The Board of Advisors is a cross industry, global body, which assists and supports the Council and its objectives, including by (a) reviewing, commenting on, and voting with respect to the Council's release of all Major Standards Work Items, (b) expressing the views and opinions of PCI Participants and the broader PCI community to the Council and PCI SSC Executive Committee (See Section 4.6.1 below), and (c) advising and providing strategic guidance to the Executive Committee regarding matters such as technical and strategic aspects of the Council's PCI Standards.

Each Advisor in Good Standing participates in all votes submitted to the Board of Advisors, on a one vote per Advisor basis.

For additional information regarding Board of Advisors eligibility, composition, Good Standing and voting requirements, and rules of engagement, please see the Charter of the Board of Advisors[6].

4.3 Regional Engagement Boards

Regional Engagement Boards (REBs) provide region specific input to the Executive and Management Committees. Each REB comprises representatives of the PCI Participants, Third Party Assessors and Affiliate Members in its applicable region, represents corresponding regional stakeholder perspectives, and provides feedback and guidance to PCI SSC on the development and adoption of payment security standards and programs in its region.

4.4 Special Interest Groups

Special Interest Groups (SIGs) are PCI SSC supervised, community-driven initiatives that focus on payment security or technology topics related to PCI SSC Standards. Involvement in a SIG enables participants to provide expertise to the Council and help develop practical payment security resources

for the industry. SIG work may contribute to clarification of specific requirements within a Standard, examine how Standards work within any given industry or environment, or produce guidance on any other area that supports the Council's mission of raising awareness and increasing adoption of the PCI SSC Standards. SIG topics are chosen by vote of the PCI Participants. Eligible participants may include Principal POs, Associate POs, Affiliate Members, Third Party Assessors, and others by invitation.

4.5 Task Forces

PCI SSC Task Forces provide PCI SSC with advice regarding specific technical aspects of the PCI SSC Standards, including as part of the development process. Depending on the Task Force, eligible participants may include Principal POs, Associate POs, Affiliate Members, Third Party Assessors, and others by invitation. Task forces typically are established to:

- Address specific technical, business, or operational matters relevant to PCI SSC standards or programs; or
- Explore new topics that may become the focus of a Working Group

4.6 PCI SSC

PCI SSC is the standards body that maintains the PCI SSC Standards and supporting programs and documentation. PCI SSC is governed by an Executive Committee and develops its Work Items and other deliverables through its Working Groups, Special Interest Groups, and Task Forces, with input from PCI Participants through RFCs, and from the Board of Advisors on strategic, business, and operational matters.

4.6.1 Executive Committee

The Executive Committee is the Council's governing body, and is ultimately responsible for the Council's strategic, corporate and operational matters, and approval of all Major Standards Work Items in accordance with this Policy. The Executive Committee is comprised of senior representatives of the PCI SSC Founding and Strategic Member companies.

4.6.2 Management Committee

The Management Committee is responsible for oversight of the operational matters for the Council, including all Standards Programs, the provision of recommendations, suggestions and guidance to the Executive Committee regarding new Work Items and operational matters, maintaining the Standards and other Work Items, and oversight of all Working Groups, SIGs, Task Forces, RFCs and other technical initiatives. The Management Committee is subject to oversight of the Executive Committee and is comprised of representatives of the PCI SSC Founding and Strategic Member companies.

4.6.3 Working Groups

Working groups are generally established on a Standard-by-Standard or program-by-program basis, to develop Standards, Other Work Items, and other Council programs and deliverables. Working Groups are comprised of designated PCI SSC Founding and Strategic Member representatives, Affiliate Member representatives (depending on the Working Group), and execute PCI SSC strategies in consultation with the Executive Committee, Board of Advisors, Management Committee, and Council management.

4.6.4 Council Management and Staff

PCI SSC management and Staff, including the Executive Director, oversee the operations and carry out the day-to-day activities of the Council and support the Council's Board of Advisors, Working Groups, SIGs, Task Forces, and other Council committees and programs.

5. Development Process

Development of Work Items is an ongoing and iterative process, with new Standards and other Work Items being launched to meet ever-changing payment security needs, and existing Standards and other Work Items being reviewed and updated, as needed.

Depending on the subject matter, Work items are developed through the combined efforts of applicable Working Groups, PCI Participants, the Board of Advisors, SIGs, Task Forces, RFCs, REBs, and Council committees and staff.

5.1 New Work Items

New Work Items (whether newly proposed Standards or revisions to existing works) are generally proposed by PCI SSC Working Groups or committees but may also be proposed through feedback and suggestions of the Board of Advisors, PCI Participants, or other industry stakeholders.

All new PCI SSC Standards are formally initiated at the Executive or Management Committee level, and designated to an existing or new Working Group for execution.

5.2 Working Groups

Working Groups, through the applicable Working Group chair, manage and implement the development process, including primary responsibility for the development of all Work Items, launching, managing and coordinating all aspects of corresponding RFCs, and liaising with PCI SSC's Board of Advisors, SIGs, Task Forces, committees, management, and others, as applicable.

5.3 Requests for Comments (RFCs) and Disposition of Comments

At applicable points in the development process, PCI SSC generally initiates Requests for Comments (RFCs) on all Major Standards Work Items, and on other Work Items as deemed necessary by the Council. RFCs provide critical feedback to PCI SSC and an opportunity for interested stakeholders to influence and participate in the development of existing and new Standards. The Working Group reviews and addresses RFC comments in accordance with the RFC Process Guide, and engages in further stakeholder outreach as needed. Depending on the RFC topic, eligible RFC participants may include subject matter experts (SMEs), PCI Participants, assessors and labs, the Board of Advisors, Task Forces, and others. For additional information see https://www.pcisecuritystandards.org/get_involved/request_for_comments/

6. Approval Process

All Work Items that complete the development process require approval prior to publication.

6.1 Major Standards Work Items

All Major Standards Work Items (i.e. New Standards and Major Revisions to Standards) that complete the development process are reviewed and approved prior to publication, in accordance with the following process.

6.1.1 Management Committee Ballot

All Major Standards Work Items must be approved by the Management Committee. See attached Schedule 2 hereto for a graphical representation of the Major Standards Work Item approval process.

6.1.2 Board of Advisors Engagement

Once a Major Standards Work Item is approved by the Management Committee, the Council initiates a corresponding Board of Advisors engagement period for that Work Item. The Board of Advisors engagement process is intended to help ensure that the Advisors are sufficiently informed regarding the Major Standards Work Item, that there is a general level of consensus that such Work Item is appropriate for ballot, and that all Advisors have received a preview of the current draft. Based on the results of this process, a Major Standards Work Item may be returned for further review, change or approval by the Management Committed or applicable Working Group, and/or subject to additional Board of Advisors engagement, as appropriate.

6.1.3 Initial Executive Committee Ballot

After completion of the process outlined in Section 6.1.2, the Major Standards Work Item is then submitted to Executive Committee ballot. If approved, the Work Item is submitted for approval of release by the Board of Advisors. If not approved, the Work Item is returned to the Management Committee or applicable Working Group for further review and disposition.

6.1.4 Initial Board of Advisors Ballot

Subject to Sections 6.1.7 and 7 below, each Advisor in Good Standing receives and is expected to exercise its vote on each Major Standards Work Item, by the applicable ballot deadline.

The ballot deadline for each Board of Advisors Major Standards Work Item ballot is generally 2 calendar weeks after the ballot is opened and will be specified in the ballot.

Voting options for all Board of Advisors Major Standards Work Item ballots are:

- Yes (means the Advisor approves the Major Standards Work Item for release)
- No* (means the Advisor does not approve the Major Standards Work Item for release)
- Abstain

*If an Advisor votes “No” at the time of ballot, the Advisor must accompany its “No” vote with comments that describe the reasons for its “No” vote and the specific changes that would be required to change its vote to “Yes” (“Acceptable Comments”)[7].

Advisors that submit “No” votes early, without Acceptable Comments, may submit their comments by the applicable ballot deadline.[8]

If the ballot deadline is reached, and an Advisor either has not submitted a vote, or has submitted a “No” vote without Acceptable Comments, the Advisor’s vote will be deemed to be an abstention and recorded as “Abstain (no vote)” for purposes of that ballot.[9]

[7] PCI to establish internal policy for determining whether comments are Acceptable Comments.
[8] PCI to confirm whether current voting technology/processes support the ability of advisors that initially enter “No” votes to change, add or supplement their initial comments.
[9] To be determined (and documented in the BoA Charter) whether a “No” vote without Acceptable Comments is counted as a vote for purposes of attendance/good standing requirements.

Approval: Major Standards Work Items approved by a majority of all Advisors (excluding abstentions and deemed abstentions) at the initial Board of Advisors ballot stage are scheduled for publication by the Council. The specific release date and support conditions, if any, are separately approved by the Executive Committee.

6.1.5 Executive Committee Review

Major Standards Work Items not approved for publication at the initial Board of Advisors ballot are subject to Executive Committee review, during which the Executive Committee reviews submitted comments and determines whether to terminate (and not publish) the Major Standards Work Item, or modify the Item and initiate an additional Board of Advisors ballot.

Major Standards Work Items modified at this stage may be returned to the Management Committee or applicable Working Group for revision, may be submitted to additional Management Committee or Executive Committee approval, and are then submitted to an additional Board of Advisors engagement process prior to being submitted for an additional Board of Advisors ballot (an "Additional Ballot").

6.1.6 Additional Ballots, Reviews and Approval

If the Major Standards Work Item is submitted to an Additional Ballot, subject to Sections 6.1.7 and 7 below, after an additional engagement period (see Section 6.1.2 above), each Advisor in Good Standing is eligible and expected to submit (in accordance with Section 6.1.4 above) its vote on the Additional Ballot.

Approval: Major Standards Work Items that are not rejected (by "No" votes with Acceptable Comments) by at least 2/3 of all eligible Advisors[10] during an Additional Ballot are deemed to be approved, and accordingly, scheduled for publication by the Council, the specific release dates and support conditions, if any, to be separately approved by the Executive Committee.

Major Standards Work Items not approved or deemed to be approved by the Board of Advisors during any Additional Ballot (a) may be subject to further Executive Committee review, (b) may be modified or terminated (and not published) in accordance with Section 6.1.5, (c) may be submitted to either an Additional Ballot or a ballot of the Executive Committee, and (d) may be published only if approved (or deemed to be approved) by a subsequent Additional Ballot or by unanimous ballot of the Executive Committee.

In the event of publication following a unanimous Executive Committee vote to publish, the Executive Committee will note the comments that accompanied "No" votes in the preceding Board of Advisors ballot, and document its rationale for the industry need for the Major Standards Work Item. Such comments, rationale, and corresponding vote counts will be made available to the Board of Advisors.

6.1.7 Board of Advisors Voting Requirements

To be eligible to vote on Major Standards Work Items, Advisors must be in Good Standing, as specified in the Charter of the Board of Advisors.

6.1.8 Ballots and Ballot Results

[10] Voting thresholds for Initial BoA Ballot and Additional BoA Ballots should be confirmed across documents.

All Board of Advisors ballots for a Major Standards Work Items are formally submitted, recorded and managed, and reviewed by the Executive Committee and Council staff. Such ballot results are shared with the Board of Advisors only after the applicable ballot deadline. Votes by voice, email or proxy are not allowed or counted except in extenuating circumstances with prior PCI SSC approval.

6.1.9 Resolution and Communication of Comments

At each stage, PCI SSC will, as applicable, review, address, and resolve to its satisfaction all comments received in accordance with the foregoing process, and communicate such comments and their resolution (if any) to the Board of Advisors, including attribution to the source of the comment.

PCI SSC reserves the right to publish any comments, provided that in doing so, PCI SSC will not attribute a given comment to a given source, and will use reasonable efforts not to publish any comment the source of which is reasonably likely to be determined from the content of the comment.

6.2 Other Work Items

Other Work Items are not normally voted upon by the Board of Advisors, and depending on the Work Item, generally require approval of the applicable Working Group, the Management Committee, and/or the Executive Committee prior to publication. Under special circumstances, as determined by the Executive Committee, Other Work Items may be submitted as ad hoc items to the Board of Advisors for voting. If an ad hoc item is submitted for Board of Advisors voting, it does not establish additional voting rights on related or similar situations.

7. Modification and Interpretation

All terms, conditions, rights, and rules of participation associated with Council initiatives and programs, including but not limited to the provisions of this Policy, are determined at PCI SSC's sole discretion and may be modified at any time. All decisions and interpretations of the Council regarding this Policy and the terms hereof shall be final, conclusive and binding on all parties and matters subject to such terms.

Schedule 1

Approval Process for Major Standards Work Items