



PA DSS Webinar FAQ

SISA's webinar PCI SSF is replacing PA DSS. What's your next step, examines the critical requirements for risk and compliance teams to shift from PA DSS to PCI SSF standard easily and exhibits cases of how our customers are evolving their approaches to this transition.

While we tried to answer all the questions and queries of our participants, we'd like to address a set of inquiries that our valued webinar attendees frequently registered through this E-book.

If you still have any questions or would like to consult with an expert, please write to us at contact@sisainfosec.com

1. Is PCI SSF control implementation possible only on applications or in specific zones as well?

PCI SSF has collectively two standards

Secure Software Standard – Secure Software Standard (PCI S3) has control objectives and modules which are implemented on Applications and Environment Configuration of Applications.

Secure Software Lifecycle Standard – Secure SLC has control objectives that defines a set of security requirements and associated test procedures for software vendors to validate how to properly manage the security of payment software throughout the software lifecycle.

Additionally, PCI S3 is applicable on payment applications entirely, and the eligibility is based upon their transaction processing capabilities and their impact on the security of payment transactions.

2. If we build a generic software for all our clients and it is later customized for a particular client, does the S3 criteria still apply for the software of that particular client?

Based on application functionality and the customization provided to the clients, during the review process, the S3 QSA will be able to assist you on whether the minimal impact change qualifies for an assessment or not. However, as per the S3 guidelines, the modules, application functionality, etc. should remain the same. It's just the interface of the application that can be customized based on the request from the customer.

3. What is the estimated approximate cost for S3 and Secure SLC Certification?

There are two payments involved for S3 and Secure SLC certifications, which are similar to PA-DSS standards.

- i. Assessment Fees are chargeable by the S3/S-SLC QSA based upon the size of the application or according to the scope of the software development practices.
- ii. Listing Fees – It will be charged directly by PCI-SSC based on the below catalog:

- S3 Certification listing fee

New Payment Software Listing Fee	USD 3,000
Payment Software Administrative Change Acceptance Fee	USD 275
Payment Software Low-Impact Change Acceptance Fee	USD 500
Payment Software High-Impact Change Acceptance Fee	USD 1,500

- SSLC listing fee

New Secure SLC Qualified Vendor Listing Fee	USD 5,000
Secure SLC Qualified Vendor Administrative Change Acceptance Fee	USD 250
Secure SLC Qualified Vendor Designated Change Acceptance Fee	USD 500

4. What compliance requirements are mandatory when an application saves users payment information but uses a payment gateway to process the payment?

If the application qualifies the eligibility criterion of S3, then all Secure Software Core Requirements and Module A (Account Data Protection) are mandatory for meeting the Secure Software Standard objectives. And, the applicability is related to any software directly supporting or facilitating payment transactions that store, process, or transmit clear-text account data.

5. Currently, under PA DSS, delta changes are categorized as High/Low/No Impact. So, how do these changes occur under the new framework?

The changes are categorized under 2 standards:

As per the PA DSS Standard, changes are differentiated by Administrative Change, High Impact Change, Low Impact Change, and No Impact Change.

As per the SSF Standard, changes are differentiated by Administrative Change, High Impact Change, Low Impact Change. However, 'No Impact Change' is not a part of the SSF Standard.

Moreover, if the Vendor is a 'Secure SLC Qualified Vendor', they can perform delta assessments by themselves (Delta Assessments consists of Administrative Change and Low Impact Change).

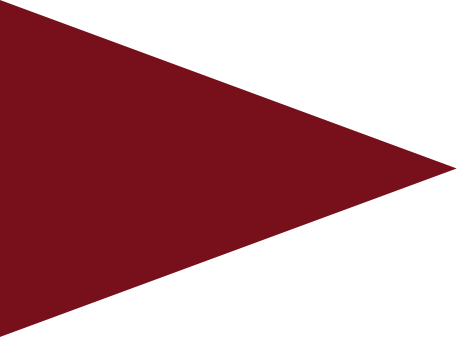
For more information, download the latest version of "Secure Software Standard"

1. Click on the following PCI Document Library link https://www.pcisecuritystandards.org/document_library

2. Filter by "SOFTWARE SECURITY" and click on "Secure Software Standard" to download

6. What about the 2021 year-end Revalidation Plan for the existing PA DSS listed application?

As per the current update from PCI SSC, Annual Revalidations/Change Impact validations such as High Impact Change, Low Impact Change, No Impact Change, and Administrative Changes) are allowed till October 2022.



7. We have a payment suite certified with PA-DSS, and we are adding one more feature to the suite. So, what will be the validation process?

We have two options to proceed.

i. PA-DSS (Easy Way): PA-QSA can validate the new feature and categorize the change under High/Low, and can accordingly update the ROV and AOV documents and submit it to PCI-SSC for listing update.

ii. PCI S3: Also, it is recommended to start fresh validations for payment suite as per the SSF Framework and certify the payment suite under PCI S3 Standard.

8. With regards to the bank, (#1) how the bank could assess and ensure the off-the-shelf application from the vendor are secured and in continual compliance with PCI (or, PA DSS). (#2), In case if the bank develops and/or customized a specific API (middleware) to communicate and/or translate data over or between payment systems, how the bank could ensure that the API would comply with secure development (or PA - DSS)?

I. It is recommended to install and configure the PA-DSS certified application as per the "Implementation Guide" and "Secure Installation Guide". This will ensure that the Payment Application has been configured as per the PA-DSS Standard/Guidance. However, the Payment Application will be assessed again as per the PCI-DSS Standards by the PCI-QSA based on the Implementation Guidance.

II. If Vendors/Banks are developing customised APIs to transmit data over Payment Systems, it is recommended to undergo PCI Secure SLC Certification for the software development organization to define mature secure software lifecycle management practices in place to ensure its payment software is designed and developed to protect payment transactions and data, minimize vulnerabilities, and defend against attacks.

9. What does the Annual Revalidation Process imply a vendor who is using an existing application?

As per the current update from PCI SSC, Annual Revalidations/Change Impact validations, such as High Impact Change, Low Impact Change, No Impact Change, and Administrative Changes, are allowed till October 2022.

10. Are the SSF guidelines finalized or in progress?

Currently, PCI Council has released the second version of PCI S3 Standard 1.1 and Secure SLC standards 1.1. However, in the future, changes/updates in both the standards are expected under the SSF Framework.

For more information, download the latest version of "Secure Software Standard"

1. Click on the following PCI Document Library link https://www.pcisecuritystandards.org/document_library

2. Filter by "SOFTWARE SECURITY" and click on "Secure Software Standard" to download

11. Do the PCI SSF standards apply to TSPs who are partners with REs, and are they supposed to get S3 or SSLC Certified? Can you please brief it along with examples?

i. For Secure Software Standard - It is aimed at payment software. The eligibility criteria for software products involved in, or directly supporting, or facilitating the payment transactions store, process, and transmit the clear-text account data. And the software products developed by the vendor are commercially available for sale to multiple organizations.

ii. Secure SLC - This aims at the software vendors who develop software products for the payment card industry. The eligibility criteria for this standard apply to all vendors that develop payment software.

Further, once you fill the scope document, it will be easy for us to confirm the application eligibility for PCI S3 and vendor eligibility for Secure SLC.

12. We keep referring to only POS machines. What about the companies developing software for ATMs (which may not necessarily be payment devices all the time) that nevertheless conduct financial transactions? So, what are the implications of missing these deadlines?

PTS Certified POS Machines are referred to only for example. It is also applicable to payment applications that are deployed inside the ATM Terminals (i.e., PCI-approved POI devices).

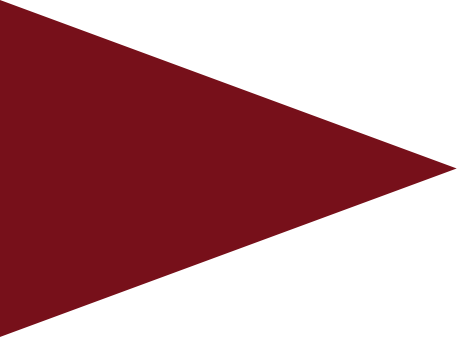
For more information, download the latest version of "Secure Software Standard"

1. Click on the following PCI Document Library link https://www.pcisecuritystandards.org/document_library

2. Filter by "SOFTWARE SECURITY" and click on "Secure Software Standard" to download

13. If I have a POS application that runs inside the Android POS App, do I need to take the PCI SSF assessment? Whether the PCI SSF and Decryption Algorithm is the same as PA DSS or not and if vulnerabilities are found in existing application architecture - is it required to change?

PCI Secure Software Standard designed "Module B - Terminal Software Requirements" applies to payment applications that are deployed inside the PCI-approved POI devices. During the review of the application, based on the application architecture and the encryption techniques, the Qualified Security Assessor will assess as per the S3 Standard Objective and will be able to guide you further if any changes are required.



For more information, download the latest version of "Secure Software Standard"

1. Click on the following PCI Document Library link https://www.pcisecuritystandards.org/document_library

2. Filter by "SOFTWARE SECURITY" and click on "Secure Software Standard" to download

14. Is it possible for organizations to apply for SLC without PCI S3 certification?

Yes, application vendors can surely apply for Secure SLC without PCI S3 Certification.

15. We have an application from the vendor who is PA-DSS certified. So, when can we ask the vendor for PCI SSF as the PA DSS certificate is valid till 30th June?

Currently, certified PA-DSS 3.2 applications are valid till October 28th, 2022. Also, it is recommended to start validating the payment application as per PCI SSF standard since it is independent of PA-DSS standard and control objectives are different.

16. Many organizations usually do audits and assessments to safeguard the apps and the infrastructures. But by increasing the scope of SSF, is it not overkilling the existing process?

Applications and Infrastructures which undergo multiple audits as per the latest requirements and standards will help vendors to reduce the "Application vulnerabilities and threats which changes with time." It also prevents and reduces the possibilities of the latest attacks and helps vendors to manage the businesses operations.

17. Question regarding the application - ecommerce application or PCI COTS certified Application – is Soft POS Application eligible for S3? Because both above applications are not intended for use on PCI Approved PTS POI Devices.

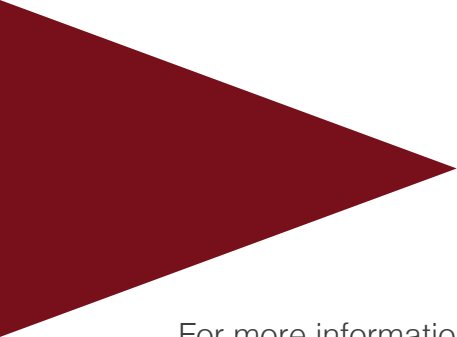
As per the current guidelines for PCI S3 eligibility, payment applications which are deployed in PCI approved PTS POI devices are eligible for S3 standard.

18. Does the existing listed PA DSS 3.2 new deployment application automatically become a pre-deployment version after Oct 2022?

Yes, after the expiration of PA-DSS 3.2 Certification on 28th October 2022, all the payment applications in "Acceptable for new deployments" will be moved to "Acceptable only for pre-existing deployments."

19. Is the protection of PII mandatory in S3 or to PAN & SAD as well?

As per the PCI S3 Standard, the vendor should identify the critical data related to the application, which is not limited to PAN and SAD. The critical data includes PAN, SAD, Tokens, Cryptographic Keys, Sensitive Functions, and Sensitive Resources along with any other data defined by the software vendor as protection required that may or may not



For more information, download the latest version of "Secure Software Standard"

1. Click on the following PCI Document Library link https://www.pcisecuritystandards.org/document_library

2. Filter by "SOFTWARE SECURITY" and click on "Secure Software Standard" to download

20. For the customers who are using our payment applications, is it necessary for them to have S3 Certification & be Compliant?

PCI S3 and SSLC Certifications are applicable for the vendors who develop the payment applications. Vendor can certify its payment application for S3 Standard or may certify its software lifecycle process with Secure SLC Standard.

21. Is it required for the Sunset Payment Applications to follow this process and get listed, or any flexibility is available?

Application validation for SSF (Software Security Standard) has started already. It is recommended to start the assessment for PCI S3 and Secure SLC to incorporate the payment application and software lifecycle process with PCI S3 Standards and Secure SLC Standards.

22. What are the needs/benefits of listing under SSLC? How does the listing happen on the PCI Side?

PCI SSC Qualified SSLC Vendor is eligible to conduct Delta assessment without Qualified Security Assessor (QSA) company. Secure SLC Qualified Vendor details will be listed on the PCI website under "Secure-SLC Qualified Software Vendor." Also, Secure SLC Qualified Vendors need not require to pay for Administrative and Low Impact changes in their application.

23. What is the timeline for SSLC? And, how to get this initiated?

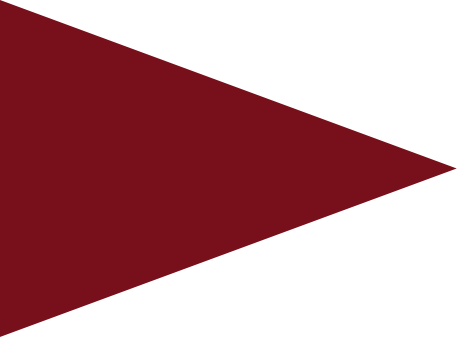
Secure SLC validations have already been initiated. The vendor can fill and share the scope document with SISA for the confirmation of the SSLC eligibility and start the SSLC listing process.

24. Is there a possibility to get re-certification using PA-DSS for already listed applications that is going to expire post-June 2021?

As per the current update from PCI SSC, Annual Revalidations/Change Impact validations (Such as High Impact Change, Low Impact Change, No Impact Change, and Administrative Changes) are allowed till October 2022.

25. What are the changes/differences between PCI DSS & PCI SSF?

PCI DSS applies to an organization that store, process or transmit the account data. Whereas, the PCI SSF Standard covers the risk factors, vulnerabilities associated with a traditional and modern payment application.



26. What should be the approach for documenting PCI-SSF?

The vendor should provide adequate documentation, pieces of evidence to SISA to confirm whether the application incorporates the requirements or not. If the application is already a PA-DSS validated one, the vendor will have most of the documents ready, and the vendor should start preparing other documents demanded by the assessor to complete the assessment. If the vendor is doing certification for the first time, it may take some time to prepare the supporting documents and understanding the requirements.

27. What is new in PA DSS, and what are the new changes as compared to the previous standard. What will happen to previous certifications and Re-certifications?

PA-DSS standard doesn't cover the latest security flaws and requirements for the latest/modern payment applications. To improve the security posture and to cover all the new attack vectors in modern and traditional payment applications, PCI SSC has introduced PCI SSF.

As per the current update from PCI SSC, Annual Revalidations/Change Impact validations (Such as High Impact Change, Low Impact Change, No Impact Change, and Administrative Changes) are allowed till October 2022. And, after the expiration of PA-DSS 3.2 certification by 28th OCT 2022, all the payment applications that are "Acceptable for new deployments" will be moved to "Acceptable only for pre-existing deployments."

28. How this affects the existing PCI DSS compliant companies?

PCI SSF will not significantly impact PCI DSS Compliance, as the SSF Standard is replacing the existing PA-DSS standard.

29. How does that affect TPAPs? Are they supposed to get S3 or SSLC certified?

As per the current PCI S3 eligibility criteria, Mobile payment applications are not eligible for PCI S3 listing. Once we have the filled scope document, it will be easy for us to confirm the application eligibility for PCI S3 standard or Vendor eligibility for Secure SLC Standard.

30. If the PA DSS certification is valid till 2023, so after 30th June 2021 what will be the status? Will, it still stay valid or it will get invalid?

All PA-DSS 3.2 certified payment applications are valid till 28 October 2022, after which all the payment applications in "Acceptable for new deployments" will be moved to "Acceptable only for pre-existing deployments." 30th June 2021 is the new deadline for submitting the documents to PCI Portal as part of the New Application listing/certification.

31. Why so much importance is being given to the date as PA DSS is getting replaced by PCI S3?

If a vendor is undergoing PA-DSS assessment for their payment application as fresh listing/certification, then the application documents should be uploaded on or before June 30th, 2021 in the PCI Portal. And, the vendor should also pay the invoice received from PCI before the above-mentioned date. PCI SSC will only complete the AQM review process for the vendors if the above criteria is met.

32. Is there any PCI SSC certification required for the developer team to develop such application?

There is no such specific certification from PCI SSC, but the vendor can opt for SSLC certification which will cover the development process of the vendor, and ultimately the developers will be aware of security processes. Vendors can also be recognized as Secure SLC qualified vendors, and the knowledge they gain in developing a secure application can also be used for developing new applications.

33. If the vendor made changes in their payment application, and we are using it as an API bind with the application. Then, how it will impact us?

Vendor should approach SISA with a "Change Impact" document to determine the impact of change in the application. As per the impact of change, the assessor will guide you - whether, a delta assessment is required or a full validation is required, and so on. The change can never be estimated until the assessor gets an in-depth understanding of the particulars.

34. Does the new SSF cover the mobile payment applications?

As per the S3 standard, a mobile application that is not solely dedicated to payment acceptance for transaction processing is not eligible. But this application can get be validated under SSLC certification.

35. By implementing Secure SDLC across the organization for all the application software we develop, will it give us any aid to self-certify on the grounds of PCI SSF?

Secure SLC Qualified vendors are eligible to conduct the delta assessment. Also, Secure SLC Qualified vendors are not required to pay any fee towards PCI Council for Administrative and Low Impact changes in their application.