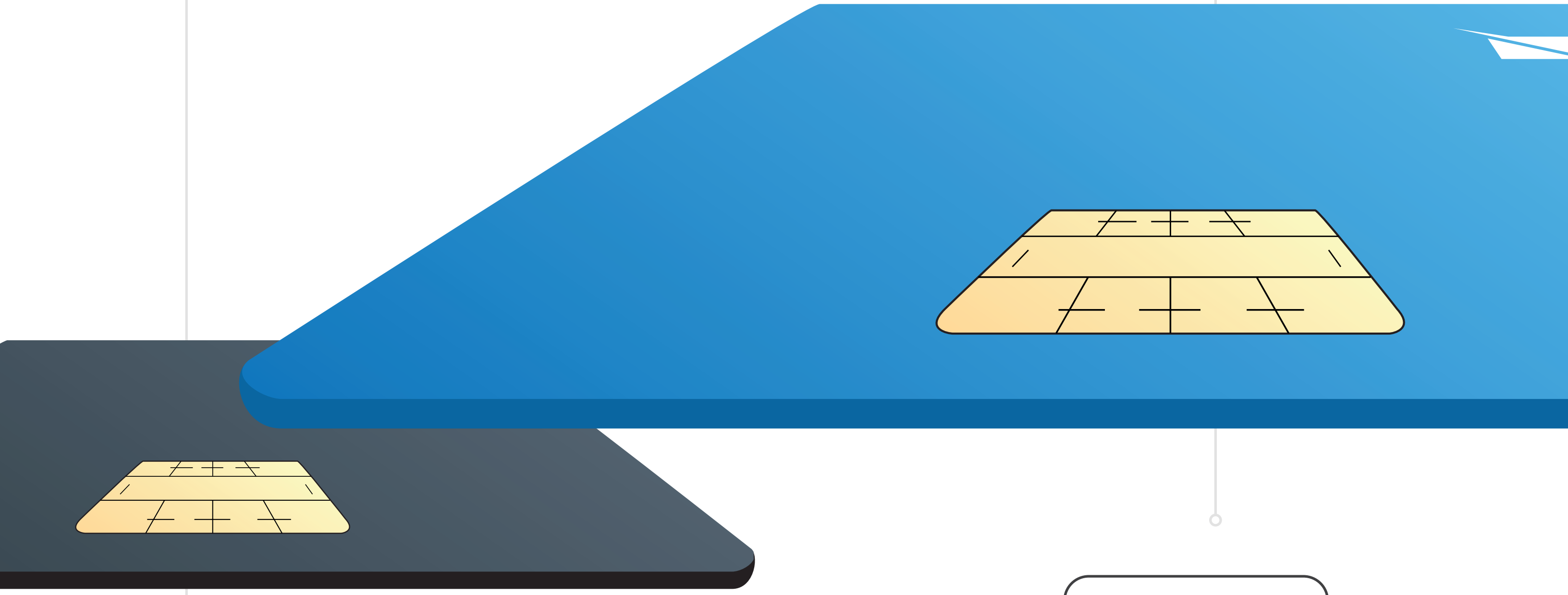
schellman
Quality, above all.



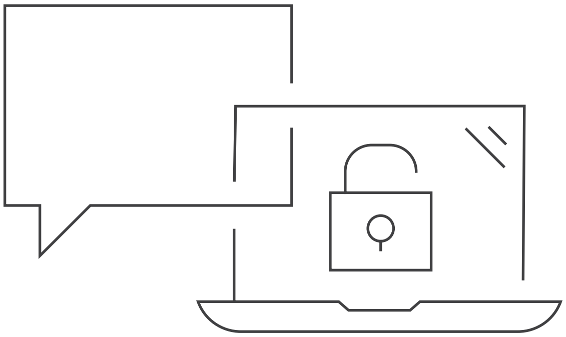
PCI SSF

Recently, Schellman & Company has become one of the first firms in the industry to offer PCI Software Security Framework (SSF) assessments as a Secure Software and a Secure SLC Assessor. As the newest application security framework published by the PCI SSC, the SSF provides an objectives-based approach to assessing the design, development, testing, and maintenance of software that handles payment card data.

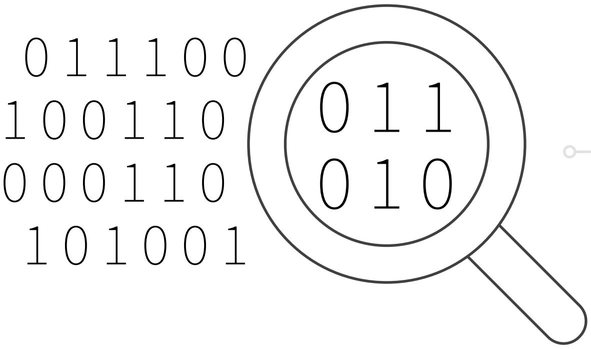
WHITEPAPER

The framework itself contains two standards:

- ***The Secure Software Lifecycle Standard*** – An interview and document-based assessment that focuses on the software development and security practices.



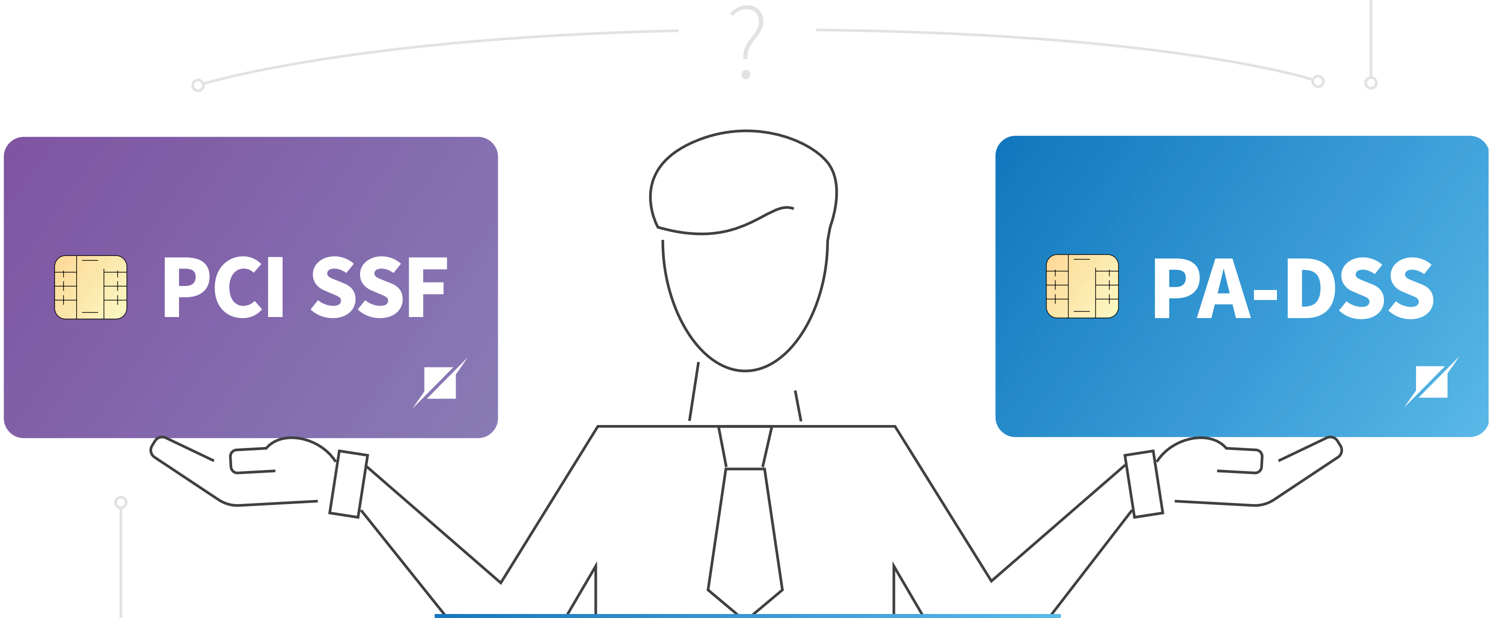
- ***The Secure Software Standard*** – Application security testing by the assessor that requires code reviews, forensic analysis, and use of static and dynamic code analysis tools.



schellman
Quality, above all.

How does the PCI SSF differ from PA-DSS?

While the PCI SSF will eventually replace the existing PCI Payment Application Data Security Standard (PA-DSS) entirely, both standards will remain in place for a while yet—PCI SSC will accept new PA-DSS submissions until June 30, 2021, and it will accept minor changes to existing PA-DSS listings until October 31, 2022. However, though both the SSF and PA-DSS focus on application security for payment accepting software, these standards significantly advance security and compliance even further than previous frameworks. With its introduction, the PCI SSF represents a more modern approach to software security and offers more flexibility for software vendors to work with their assessors to determine the best means of achieving the objectives in the standards' documents instead of using more prescriptive requirements.



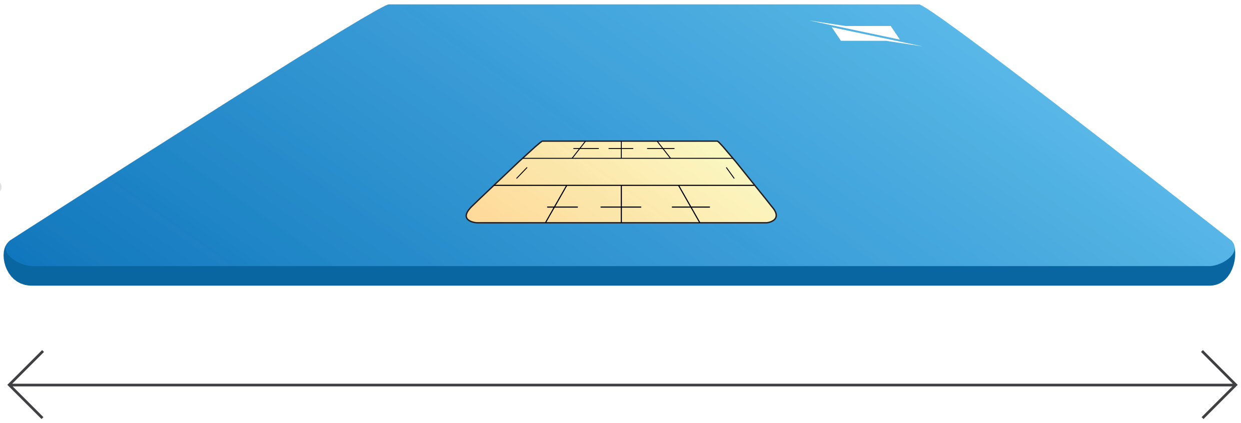
WHITEPAPER

More Flexibility

Now, within the PCI SSF, entities can meet these control objectives in a manner of their choosing and can interpret terms like reasonable or periodic by performing adequate risk assessment to justify their positions, though all interpretations remain subject to the assessor’s approval. To be clear, no one should regard this as a relaxed approach to software security, when in fact the control objectives in the PCI SSF will very likely require more activity and maturity in software security practices than PA-DSS or PCI DSS has to date.

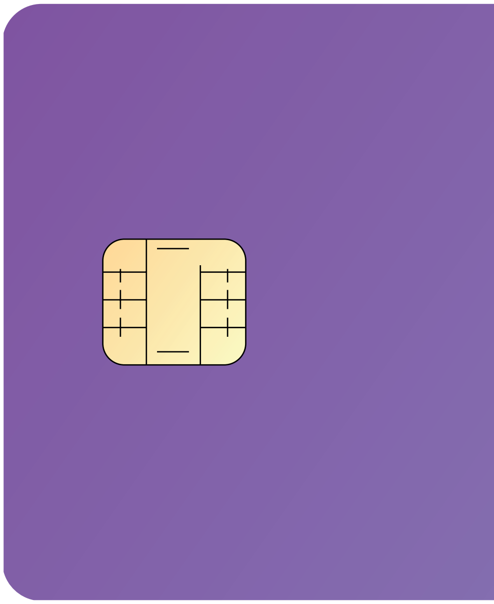
Wider Eligibility

Not only does the PCI SSF provide a new, more flexible approach, it also has somewhat broader eligibility criteria with new significant inclusions. Perhaps most interesting is that PCI SSF does not require the application to operate on the premises of the merchant or service provider who uses the application, meaning that its Secure Software Standard now allows for web applications, Application Programming Interface (APIs), or software as a service (SaaS) applications to be assessed. Furthermore, the categories for software tested under this standard have been expanded to include Payment Component alongside all the more familiar categories included in PA-DSS, such as POS Face-to-Face (i.e., a point-of-sale system intended for customer-facing card-present interactions). The new addition of Payment Component intends to apply to software components that support payment functions, even if not handling payments directly.



Impact to PA-DSS Vendors

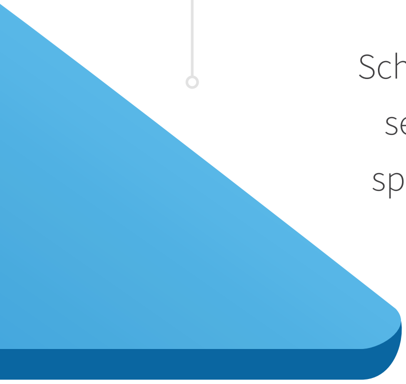
Organizations that have applications validated under PA-DSS should start considering now how they're going to make the transition to SSF and consider at least undergoing the Secure SDL assessment in 2020 in order to get the process started. As this standard focuses on the process and documentation of software development practices, an organization that undergoes the SDL assessment and is listed on the PCI SSC's list for such can perform certain low-impact changes on any listed applications under the Secure Software Standard without the involvement of their assessor—a significant benefit worth considering.



Beyond PA-DSS & Looking Forward

Even organizations who develop software that is ineligible for PA-DSS—hosted web applications and the like—should still strongly consider the PCI SSF standards in addition to their PCI DSS validation as a service provider. Because these new standards demonstrate an advanced level of maturity and comprehensiveness in their software security practices, they are able to provide better assurances regarding how assessed products and services protect payment data and other critical data assets.

For more information on the PCI SSF, its constituent standards, the Secure SDL Standard and the Secure Software Standard, please contact us at pci@schellman.com. The PCI SSF standards documents themselves are available here.



Schellman also supports a broader range of application security services, including penetration testing, ISO 9001, and sector-specific assessments in healthcare and financial technologies.

CLICK FOR MORE INFO

schellman
Quality, above all.

www.schellman.com
4010 W Boy Scout Blvd, Suite 600
Tampa, FL 33607
1.866.254.0000

Outside of the United States,
please dial: +1.973.854.4684