PCI DSS Version 4.0 is expected to be released by the end of 2020. The mandatory implementation will most likely be targeted at the end of 2021 for all the organizations that process, transmit or store payment card data. In the meantime, the current PCI DSS v3.2.1 is valid till the end of 2021.

UIT Compliance Services is responsible for PCI DSS compliance at Stanford. As a member organization of PCI Council, UIT Compliance Services is participating in the on-going PCI DSS v4.0 Draft review. Our feedback will be well factored into the proposal update process.

Currently UIT Compliance Services is reviewing the first PCI DSS Draft v4.0 for providing feedback to the PCI Council. There will be a second v4.0 Draft for our reviewing in mid 2020.

Once the PCI DSS v4.0 is published, UIT Compliance Services will perform a gap analysis for our environment for implementing PCI DSS v4.0 in 2021.

In PCI DSS v4.0, the basic 12 PCI DSS requirements remain unchanged. Fundamentally the intent of v4.0 Draft is to provide at least the same level of rigor as the existing v3.2.1 requirements to meet the security objectives.

As one of the major changes in v4.0 Draft, Compensating Controls is replaced by Customized Validation for the flexibility of reporting format and assessment. For performing Customized Validation, a company must provide details of the implemented controls that explain what is implemented and how the company has determined that the controls meet the intent of a PCI DSS requirement. The ISA or QSA assessors must use the information within the controls matrix to plan and prepare for the assessment. The controls matrix does not replace the need for the assessors to develop appropriate testing procedures for validating the implemented controls. The ISA or QSA assessors must still perform the necessary testing to verify the controls meet the intent of the requirement, are effective, and are properly maintained. Like Compensating Control, Customized Validation must be performed on a case-by-case basis for a specifically needed PCI DSS requirement, but absolutely not an over-arching approach for all the PCI DSS requirements. The Customized Validation controls matrix also does not replace the SAQ or ROC reporting requirements for customized validations.

For any questions about PCI DSS v4.0, please contact pci-compliance@stanford.edu.