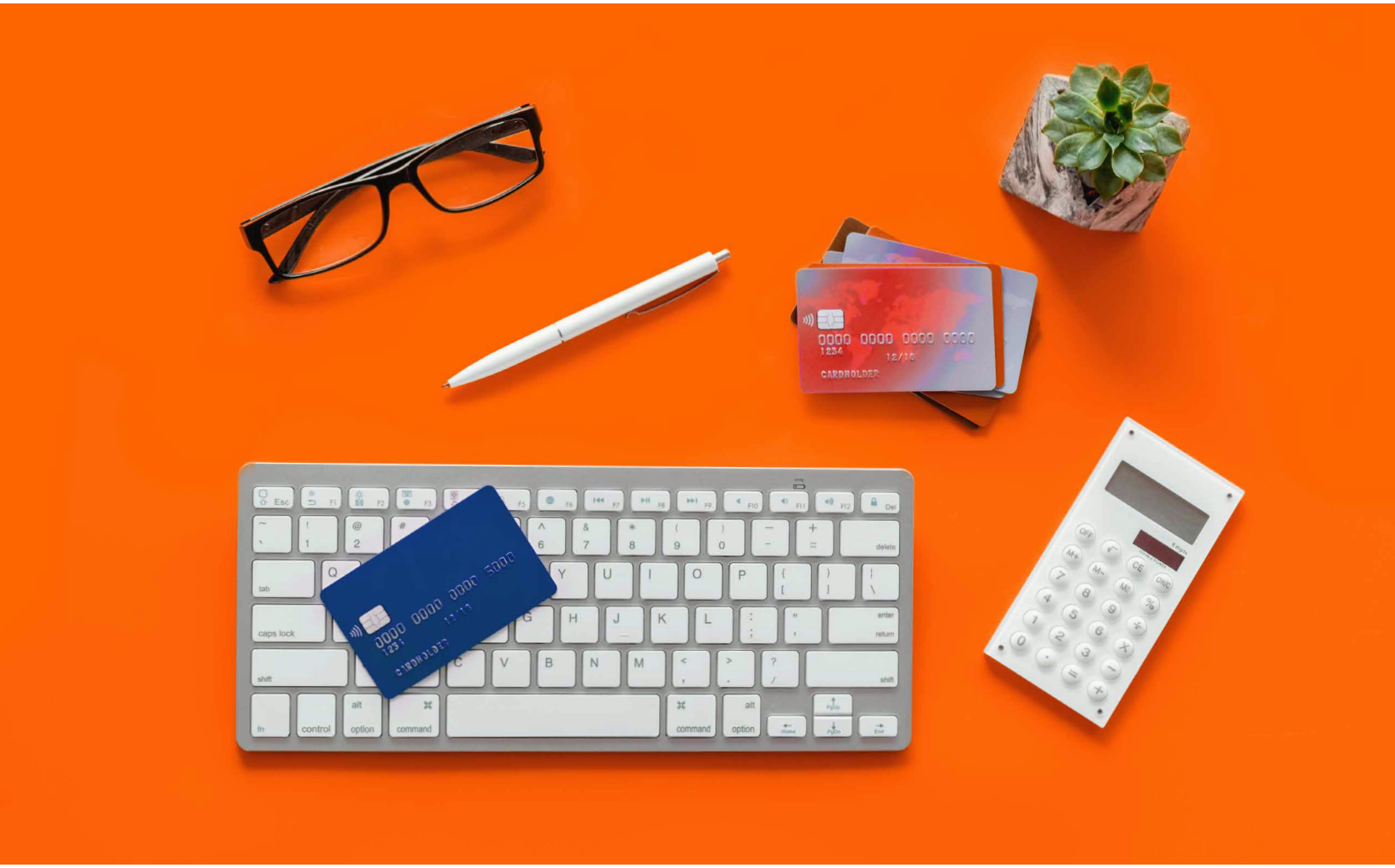


ARMOR BULLETIN – RETAIL: FALL 2020

UPDATES ON PCI DSS

The release of PCI Data Security Standard version 4.0 will constitute the most exhaustive and important update to the standard in its history.

As a cybersecurity software company specializing in securing sensitive applications and data in Cardholder Data Environments (CDE), Armor has been receiving more questions on PCI DSS v4.0 and what it means for organizations. We are providing this bulletin to bring organizations up to speed on the latest status of PCI DSS v4.0.

WHEN WILL V4.0 BE RELEASED?

The PCI Security Standards Council announced that it will release PCI DSS v4.0 in mid-2021. Additional supporting documentation will follow in the subsequent six months after its release.

REQUEST FOR COMMENT (RFC) PROCESS

The PCI Council opened a second RFC period from Sept. 23 to Nov. 13, 2020. The first draft review, held a year ago, generated more than 3,200 comments.

WHEN DO YOU NEED TO COMPLY WITH THE NEW VERSION?

The PCI Council will have an 18-month extended transition period for organizations to make the shift to the new standard once final documents, templates, and training are released at the end of 2021.

WHAT TO EXPECT WITH PCI DSS V4.0

PCI DSS v4.0 represents one of the most significant updates to the framework in its history. There has been a lot of discussion on what v4.0 will change or include. We've captured the major items below. Keep in mind that until the final standard is released in 2021, anything can change.

CLOUD SECURITY AND COMPLIANCE

We expect that cloud security will be incorporated into PCI DSS v4.0. However, given the rapid pace of change in both public cloud capabilities and adoption, the PCI Council will have to provide greater guidance that addresses the numerous cloud platforms (IaaS, PaaS, Serverless, Containers, etc.) and how organizations use them. This is no small task and may partially explain why the PCI Council has changed its approach in terms of "customized implementation," "customized validation," and a focus on outcomes.

CUSTOMIZED IMPLEMENTATION

If you are familiar with "compensating controls," the PCI Council wants you to see "customized implementation" as its next evolution. Customized implementation means that organizations can implement whatever control they want, so long as that control achieves the required outcome or intent of the requirement. It is important to note that in these circumstances, Qualified Security Assessors (QSAs) will need to conduct testing to validate that the control does work. Any testing the QSA develops is referred to as "customized validation." Depending on the extent of any customized development of testing, organizations may experience longer and more expensive audit engagements as a result. The QSA makes the call on what you did and whether it satisfactorily meets the control.

Like the current version, v4.0 will include guidance—though the approach is changing—for meeting requirements that organizations can follow. It is just not clear to what extent this guidance will address the many use cases of organizations operating in the cloud.

PRESCRIPTION VS. DESCRIPTION

With v4.0, the PCI Council is shifting the focus and intent of its guidance in addressing controls, making them less prescriptive and more descriptive. This lends itself to the flexibility needed as public cloud adoption rises and we see more cloud-based use cases—not to mention the evolution of more complex hybrid and multi-cloud environments.

FOCUS ON OUTCOMES

The PCI Council is also changing its language with v4.0, with more focus on achieving security outcomes. In practice, this would mean that instead of a focus on implementation of a specific control, the focus is on the outcome any applied control achieves. This, in addition to emphasis on the intent behind each requirement, gives more flexibility to organizations as they go about their efforts in meeting the framework.

ACCESS MANAGEMENT

There will be changes around the use and specification of passwords in v4.0. Part of this is to align with National Institute of Standards and Technology (NIST) and other frameworks' stances on access.

DATA SECURITY

Indications are that the PCI Council is strengthening practices around data security, including encryption of data in transit even within a trusted environment.

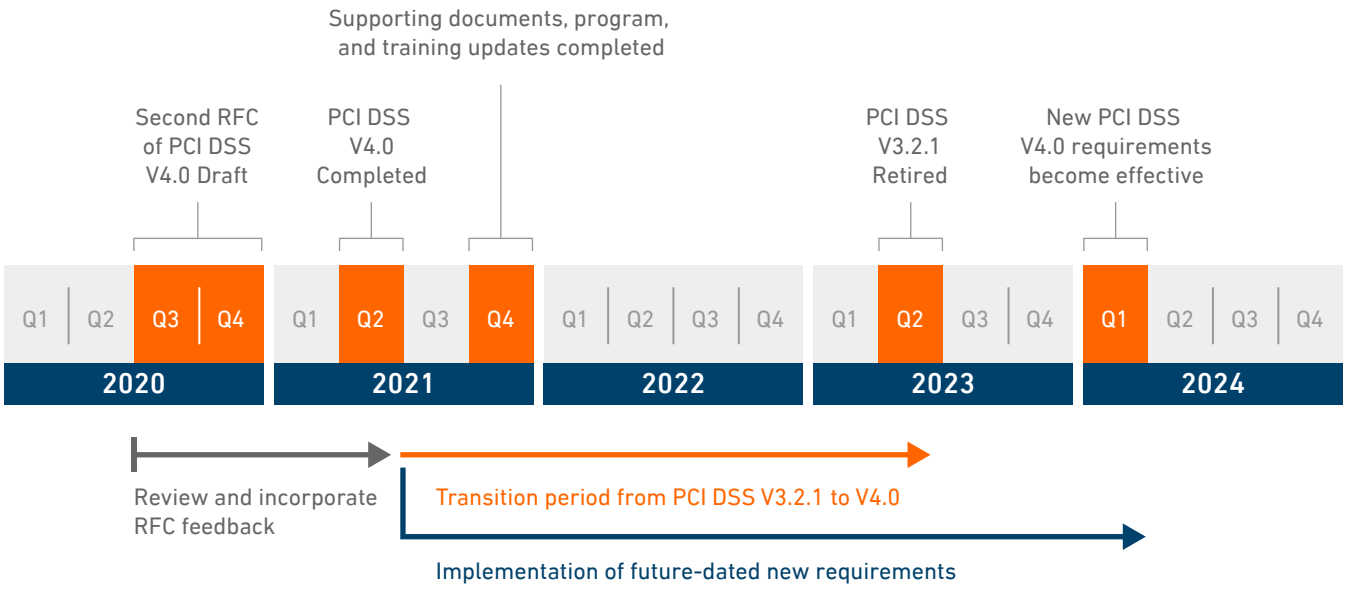
CONTINUOUS COMPLIANCE

PCI DSS v4.0 also places more emphasis on compliance being a continuous process. This is an important emphasis especially as technologies such as Cloud Security Posture Management give organizations the ability to automate and evolve their compliance with PCI DSS as they adopt the public cloud.

LONGER & MORE EXPENSIVE AUDITS

As we alluded to earlier, the use of "customized implementations" to address controls means that audits could become longer and more expensive. Because QSAs are on the hook for determination of whether a control satisfies a requirement, the QSA has an incentive (to avoid risk to the QSA company) to develop tests that effectively validate the custom control. The more customized implementations you use to address requirements, the longer and more expensive you can imagine your audit engagement.

PCI DSS V4.0 DEVELOPMENT & TRANSITION TIMELINE



All dates are subject to change.

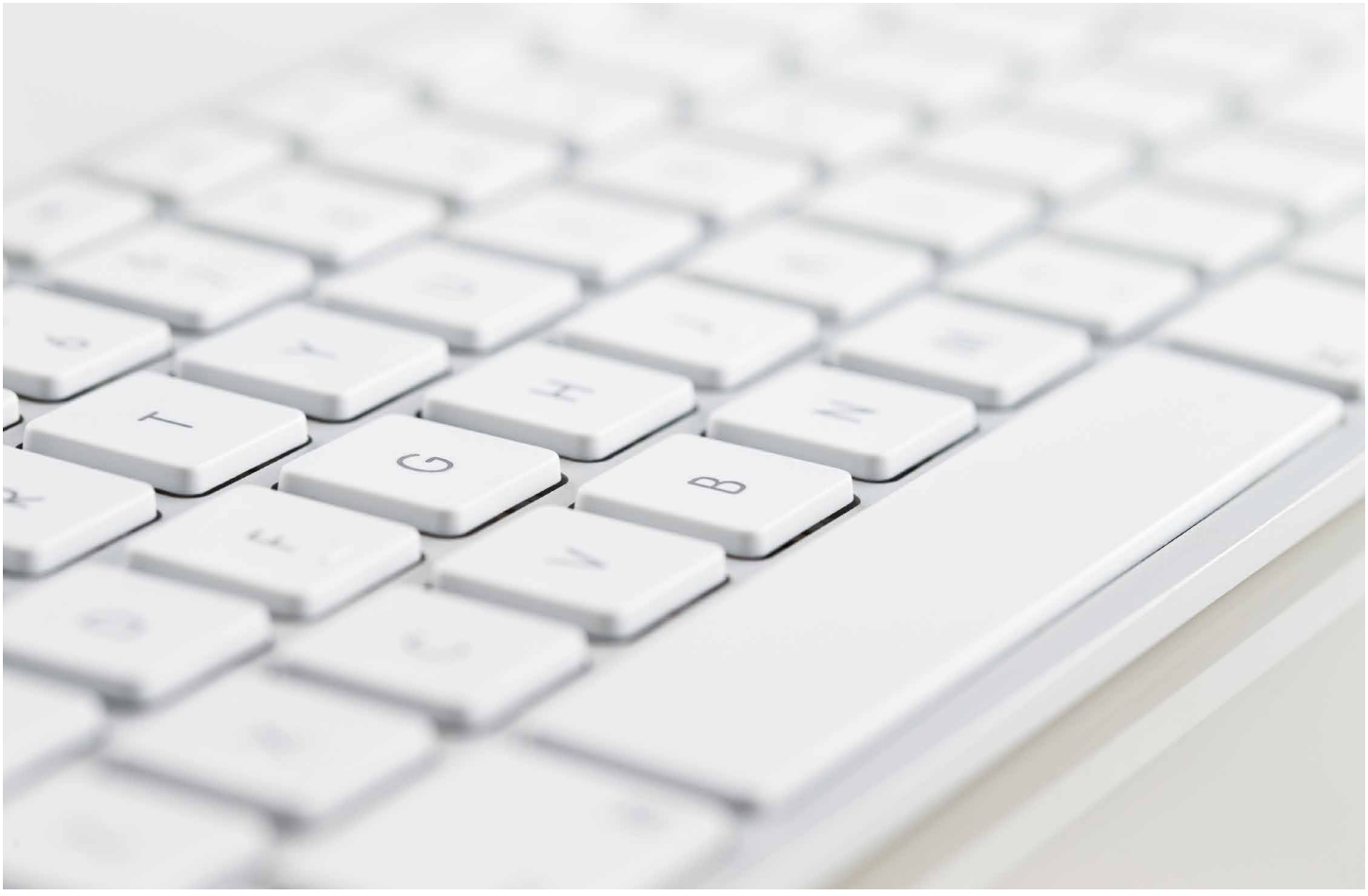
ABOUT ARMOR

Armor is a global cybersecurity software company. We simplify protecting data and applications in private, public, or hybrid clouds as well as help organizations comply with major regulatory frameworks and controls. We know security is complex; it doesn't have to feel that way.

To accelerate your compliance with PCI DSS now and in the future, check out Armor.com.

SOURCES:

- Gray, L. (2019, September 18). *5 questions about PCI DSS v4.0.* PCI Security Standards Council. https://blog.pcisecuritystandards.org/5-questions-about-pci-dss-v4-0
- Malone, A. *Insights, information and practical resources to help your organization protect payment data.* PCI PERSPECTIVES.
- Holloway, L. (2020 July 29). *A view into feedback from the PCI DSS v4.0 RFC.* PCI Security Standards Council. https://blog.pcisecuritystandards.org/a-view-into-feedback-from-the-pci-dss-v4-0-rfc



ARMOR.COM | (US) +1 844 682 2858 | (UK) +44 800 500 3167