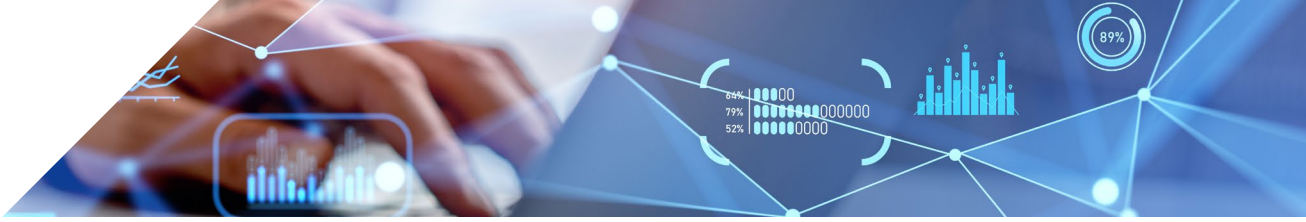
PCI DSS 4.0 Is Here
Are You Ready?

In 2006, major card brands such as Visa, MasterCard, American Express, Discover, and JCB International came together to establish the PCI Security Standards Council (PCI SSC or the Council) with the aim of establishing a global standard for credit card data security. Throughout the years, there have been periodic revisions and updates to these standards to further clarify and increase payment security measures for merchants. Since version 3.2.1 went into effect in 2018, the landscape has undergone significant changes — marked by a surge in online payments and the rapid digital transformation brought about by the global pandemic. Business networks are shifting from traditional on-premises data centers with routers, switches, and servers to cloud-hosted containers.

Given the inherent and continually evolving risks associated with the digital transmission of cardholder data across the payment lifecycle, the Council is committed to adapting the standards to address contemporary data protection requirements. In this article, we break down the biggest changes going into effect and how telecom companies should prepare for this transition.



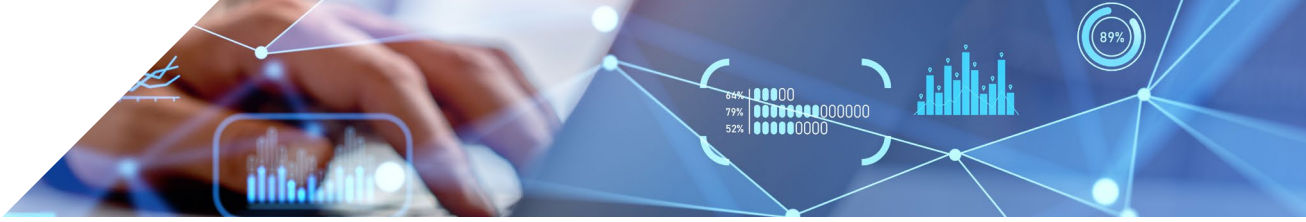
What's New With PCI DSS 4.0?

While the 12 core requirements are fundamentally similar to the previous version of PCI, the new version has an increased focus on security objectives, aiming to deliver flexibility through customization options, advocate for continuous security, and improve user authentication mechanisms. Here are some of the biggest changes you can expect with PCI 4.0:

Customization for Flexibility: In the previous iteration of PCI DSS, merchants and service providers faced a complex process when unable to meet specific controls. PCI 4.0 introduces a more flexible approach with customized controls. Organizations can now indicate the use of a new control, marked as customized, simplifying the assessment process and offering increased flexibility for risk-mature organizations to achieve compliance. The customized approach acknowledges the possibility of multiple routes to achieve security objectives and allows organizations to innovate, provided they can prove to an auditor that their approach effectively meets these security goals.

Enhanced Authentication: In today's cloud-centric environment, controlling data access through robust identity and access management is crucial. PCI DSS 4.0 aligns with zero trust principles, emphasizing multifactor authentication (MFA) for all accounts with cardholder data access, regular password updates, stronger password requirements, periodic access privilege reviews, and careful monitoring of vendor and third-party access. Additionally, the Council clarified what constitutes as MFA – noting that using a single factor twice is now called out as unacceptable.

Expanded Encryption and Data Discovery: The demand for enhanced cardholder data security standards has grown significantly, primarily due to the rise in cyberthreats involving malicious code. This presents a significant challenge for financial institutions and e-commerce as this code, once infiltrated into the network, can be exploited to access cardholder data during transmission. PCI 4.0 addresses this specific concern by broadening the scope of cardholder data encryption on trusted networks and offering best practices and valuable guidance on safeguarding network transmissions effectively.



Technology Advancement Requirements: PCI DSS 4.0 adopts a more risk-focused approach amid rapid technological advancements, enabling adaptable information system solutions that streamline processes while ensuring compliance. This version enhances security by mandating multi-factor authentication for all credit card data access, not just remote access, requiring encryption of stored authentication data, previously only recommended in 3.2.1. Having a web application firewall (WAF) to protect websites against malicious web attacks is no longer optional but required in PCI DSS 4.0.

Shift to Continuous Compliance: PCI DSS 4.0 recognizes the need for ongoing compliance rather than treating it as a one-time assessment. It emphasizes security-by-design, vulnerability assessments, real-time monitoring, and reporting to enable organizations to demonstrate compliance seamlessly whenever assessed, aligning with a continuous compliance approach.

When Does PCI 4.0 Go Into Effect?

Of the 63 new requirements, the initial 13 are lower effort as they're similar to current requirements and must be met by the initial deadline of March 31, 2024, while the remaining 50 become enforceable exactly a year later. The impact of these new requirements will vary among organizations, depending on their unique complexities. Organizations with intricate or diverse technology stacks in their payment processes will likely face the most significant impact. We're getting closer to the deadline, so if you haven't already started prepping for this change, now's the time.

How Telecoms Can Prepare For The Shift

PCI DSS 4.0 marks a significant update, but there's no need for companies to feel overwhelmed. While these fresh regulations represent a notable evolution, the core framework of PCI DSS compliance remains largely unchanged. Organizations that are used to regulatory compliance will find the language in the new regulations quite familiar.

To begin preparing for these shifts, businesses should take time to really understand the new standards, conduct a gap assessment to identify what's not currently in place, and prioritize the changes needed. Once you understand what changes are needed, consider your organization's security strategy and approach to risk management to determine which validation approach is best. The defined approach adheres to the standard method outlined in the PCI DSS requirements and testing procedures, while the new customized approach permits organizations to create personalized security controls to fulfill customized approach objectives. If opting for the customized approach,

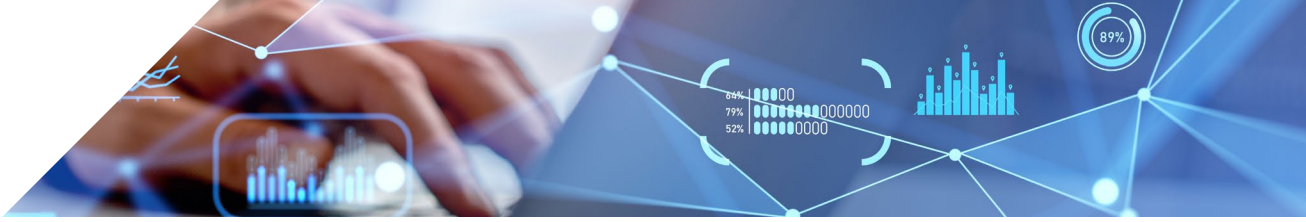
it's crucial to have a deep understanding of the requirements and ensure that your implementation aligns with the added risk analysis and documentation prerequisites before proceeding with validation.

One of the biggest, over-arching changes to the new standards is the shift to a continuous, organization-wide compliance model. It's important to include additional training and education for users and stakeholders in your transition plan. Once the entire team understands the new PCI objectives, organizations can assign and define explicit roles and responsibilities for anyone interacting with cardholder data or account information, with clear communication and individual acknowledgment, as this alignment among stakeholders is instrumental in successfully navigating the PCI assessment process.

Building a More Secure Future With IDI

Meeting the updated PCI 4.0 requirements may pose challenges, but it's a vital move that opens doors to new business prospects, partnerships, and ultimately builds better user experiences. With rising security concerns, telecom service providers must be vigilant about their security compliances to ensure their customers' data is protected. An important part of that is ensuring their partnering organizations are held to the same security standards.

As a leading Billing & OSS solution for telecom service providers, IDI houses vast amounts of customer data. We serve as a dedicated partner and are committed to safeguarding our customers' systems and important information by regularly reviewing the threat landscape, the regulatory environment, and our customer's needs to continually enhance our security posture while providing exceptional service.



As business needs, regulations, and the risk management landscape are ever-changing, IDI continues to invest in new security practices to stay ahead and maintain a strong security program. To demonstrate this commitment, IDI started early in 2023 to understand the new PCI framework and ensure we could meet the new standards and remain compliant to better serve our customers.

Build A Better Security Experience With IDI.

Through innovative technology, people, partners, and systems, IDI is committed to providing a highly secure, world-class, cloud-based B/OSS platform, along with the insightful counsel and specialized expertise required to help you navigate the modern digital landscape.

As the telecom industry continues its rapid evolution, IDI's commitment to customer security remains at the forefront of everything we do — and that includes upholding current and future global industry standards. Talk to us today to learn more about IDI's compliances and how we protect our customers.

Call **888.924.4110**, or contact us **here.**