

The SISA logo is located in the top right corner. It consists of the letters "SISA" in a bold, white, sans-serif font. The background of the entire cover features a dark green to black gradient with dynamic, flowing, wavy lines in various shades of green that create a sense of motion and depth.

SISA

SISA CANVAS

CYBERSECURITY
CONVERSATIONS FOR A
SAFER TOMORROW.

A solid green horizontal bar spans the width of the page, starting from the left edge and ending just before the text block on the right. It has a thin white vertical line at its right end.

EDITION 4

Strategic Approaches to
Mastering Compliance with
PCI DSS 4.0 Standards

TABLE OF CONTENTS

01

From the CEO's Desk	03
----------------------------	-----------

02

Conversations with Industry Experts	04
--	-----------

Jeremy King – Regional Head, PCI SSC – Europe	05
---	----

Dawood Behbehani – AGM InfoSec – Privacy & Anti-Fraud, Kuwait International Bank	10
--	----

Sam Butler – CISO, PayU, UK	13
-----------------------------	----

03

SISA Perspective	15
-------------------------	-----------

01

From the CEO's Desk

In an era marked by rapid technological advancement and evolving threats, the importance of securing sensitive data has never been more critical. From political instability and natural disasters to economic challenges and cybercriminals wielding AI-powered tools, organizations across industries are under constant pressure to protect their assets. Nowhere is this pressure more acute than in the world of digital payments, where the value of customer payment credentials makes financial institutions and payment processors attractive targets for cyberattacks.

But it's not just the financial sector that is vulnerable. Any organization that processes payments is exposed to growing threats as digital transactions increase and attackers become more sophisticated. This makes securing customer data not just a compliance obligation, but a business necessity. Recent high-profile data breaches have highlighted the devastating consequences of failing to protect sensitive information, with 26% of consumers abandoning brands due to concerns over data security in the last year alone.

With the global digital payments market projected to grow from \$89 billion in 2022 to \$200 billion by 2030, the stakes are higher than ever. Organizations must balance the convenience of digital transactions with the imperative to protect customer privacy and data. This is where PCI DSS 4.0 comes in.

Introduced by the Payment Card Industry Security Standards Council (PCI SSC), PCI DSS 4.0 is a comprehensive update designed to address the new realities of the digital world. It builds on the foundations of previous standards but raises the bar significantly, introducing 64 new requirements to tackle evolving risks in payment security. This updated standard encourages organizations to adopt new technologies and innovative security approaches, empowering them to select the most effective methods for safeguarding cardholder data—provided they can demonstrate their effectiveness.

At SISA, we recognize the crucial role that PCI DSS 4.0 plays in protecting customer data and setting new benchmarks for security best practices. Compliance with this standard is not just about meeting regulatory requirements; it's about establishing a robust, future-ready security framework that aligns with the fast-paced innovation in the payments industry. The deadline for compliance with PCI DSS 4.0 may be March 2025, but organizations must begin their journey now,



02

Conversations with Industry Experts





Jeremy King

Regional Head,
PCI SSC – Europe

Considering most requirements don't become mandatory until March 31st, 2025, what are the timelines organizations should consider, and how can they stay relevant and updated with the changes in the services provided by the PCI DSS standard?

The timeline for implementing PCI DSS version 4.0 was quite specific. We officially released the standard in 2022, and the retirement of version 3.2.1 is now complete. Organizations must migrate to version 4.0 to maintain compliance.

The council aims to provide ample time for organizations to adapt to new standards. After the release of version 4.0 in 2022, we allowed a significant period for checking, planning, and gap analysis. Even with the release of the new version, there's an additional year before most new requirements become mandatory. Some requirements are marked as best practices

until March 31, 2025, giving organizations time to migrate without immediate pressure.

To support organizations during this transition, we offer extensive resources. Our website features a comprehensive FAQ section and numerous resources under the "resources" tab, providing detailed information on PCI DSS version 4.0. Updated supporting documentation, including self-assessment questionnaires, highlights new requirements and their implementation timelines.

We also provide a quick reference guide, blogs, and podcasts from council staff that explain the changes. These resources are designed to be user-friendly and accessible, ensuring that organizations can easily navigate the transition.

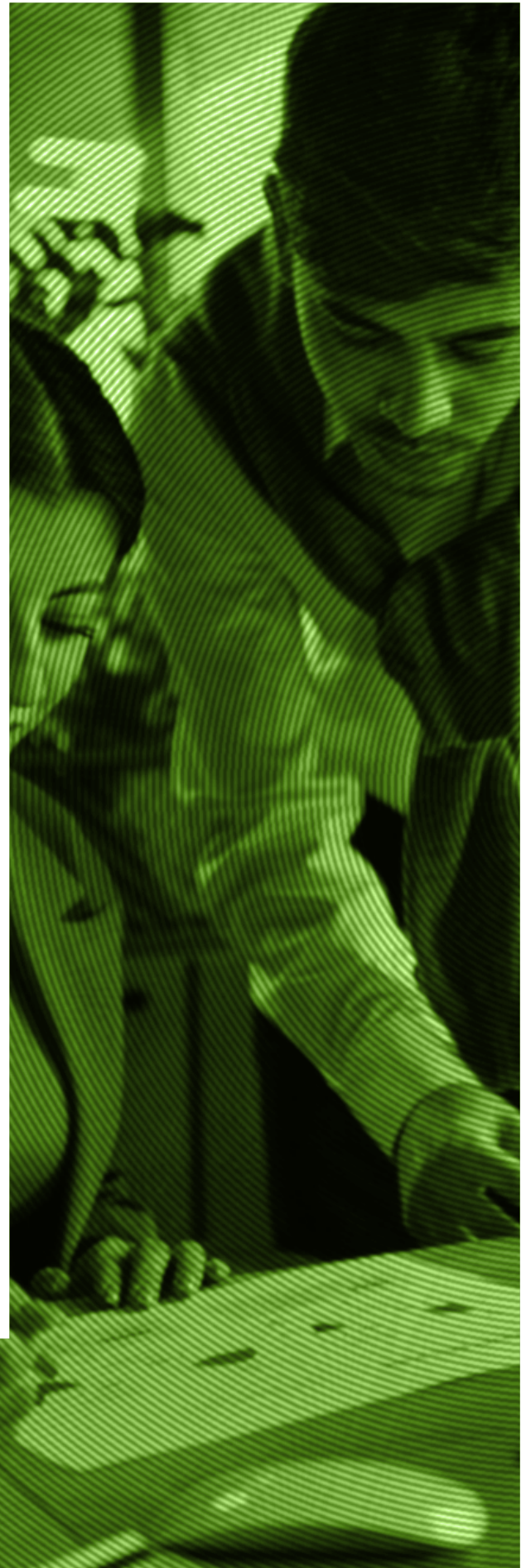
Organizations should work with their Qualified Security Assessor (QSA) as soon as possible to complete their migration to PCI DSS 4.0. This will ensure they continue to meet PCI DSS standards and protect cardholder data effectively.

Why has the trend of targeted risk analysis (TRA) become prominent, and what should organizations consider when implementing it?

Targeted risk analysis is a key aspect of PCI DSS 4.0, especially with the introduction of the customized approach. This approach allows organizations to demonstrate that they meet the intent of a requirement, even if they cannot specifically meet it using the defined approach. The purpose of TRA is to focus sharply on a particular requirement to convincingly show the Qualified Security Assessor (QSA) that the organization is seriously addressing and meeting the intended security measures.

When an organization opts for a customized approach, TRA helps confirm that this approach achieves the required level of security. It provides all necessary information for the QSA to verify that the analysis has been conducted thoroughly. Additionally, TRA has another application within the standards: it guides the frequency of security checks and tests. This guidance supports the QSA in validating that the security measures are implemented as expected.

TRA is a powerful tool within PCI DSS version 4.0. It not only supports the customized approach but also offers flexibility in how certain security activities are performed, thereby helping organizations align with the overarching goals of PCI DSS 4.0—enhancing flexibility and ensuring that organizations can effectively meet the intent of each control.



With PCI DSS 4.0, there has been a significant emphasis on application-level security, including automated monitoring solutions for all external-facing web applications. Can you explain the trend behind this focus and whether it's just for external applications or all applications within an organization?

As the world increasingly relies on software and APIs, unfortunately, so do cybercriminals, necessitating heightened security measures. From the PCI Council's perspective, any software that stores, processes, or transmits account data, or could impact the security of account data, falls within the scope of PCI DSS. This means that not only external-facing applications but all applications that could influence the security of account data need to be considered.

The necessity for robust application-level security arises from the frequency and sophistication of attacks targeting business logic. These attacks often involve attempts to manipulate APIs, communication protocols, and channels to abuse or bypass application features and functionalities. The rise in vulnerabilities, particularly in third-party components such as libraries and APIs embedded in software, presents new opportunities for criminals to infiltrate systems and access sensitive cardholder data.

Entities must ensure that all relevant software is properly configured and securely implemented to support applicable PCI DSS requirements. This includes monitoring the availability of security patches for third-party components and implementing them promptly. Delays in applying security patches can extend the window of opportunity for criminals, making timely patching a critical aspect of maintaining security. Thus, the enhanced

focus on application-level security in PCI DSS 4.0 is crucial for protecting against these evolving threats and applies to all relevant applications within an organization, not just those that are external-facing.



PCI DSS 4.0 implements more stringent controls on the management of application and service level accounts, how critical is this trend for organizations in the payments industry, and what are the key strategies for ensuring their security?

The evolution of PCI DSS reflects the growing need to enhance security measures not just to keep criminals out, but also to control their movements and potential damage if they manage to infiltrate an organization. Historically, a significant focus was placed on securing administrator accounts, which often had a common password across the organization, making them prime targets for criminals. Recognizing this vulnerability, the council mandated unique identifiers for administrators and subsequently introduced more rigorous controls.

The introduction of multi-factor authentication (MFA) for remote access was a critical development. Initially, this was deemed necessary because passwords alone were not sufficient to secure access against sophisticated cyber-attacks. Over time, as phishing attacks and credential theft became more prevalent, the need to expand MFA to include all users and all access points became apparent. This strategy significantly complicates the ability of criminals to move laterally within an organization if they gain access.

Moreover, recognizing the ongoing reliance on passwords in some organizations, PCI DSS 4.0 has responded to changes in technology and password usage by increasing the requirements for password complexity. This includes recommendations for longer passwords or passphrase usage, which are easier to remember and harder to crack.

Overall, managing application and service level accounts is crucial in the payment

domain because these accounts often have access to sensitive cardholder data. The strategies laid out in PCI DSS 4.0 aim to ensure that these accounts are as secure as possible, minimizing the risk of data breaches and maintaining the integrity of the organization's security posture. This holistic approach to account management, combining unique user identification, robust access controls, and advanced authentication measures, is essential for protecting against the evolving landscape of cyber threats.



With PCI DSS version 3.2.1 having expired, why should businesses transition to version 4.0, considering the complexity of technologies and threat landscapes?

This is one of the most common questions we receive. I recommend discussing it with your acquirer and working with your Qualified Security Assessor (QSA) to create a roadmap for your organization to achieve compliance under PCI DSS 4.0.

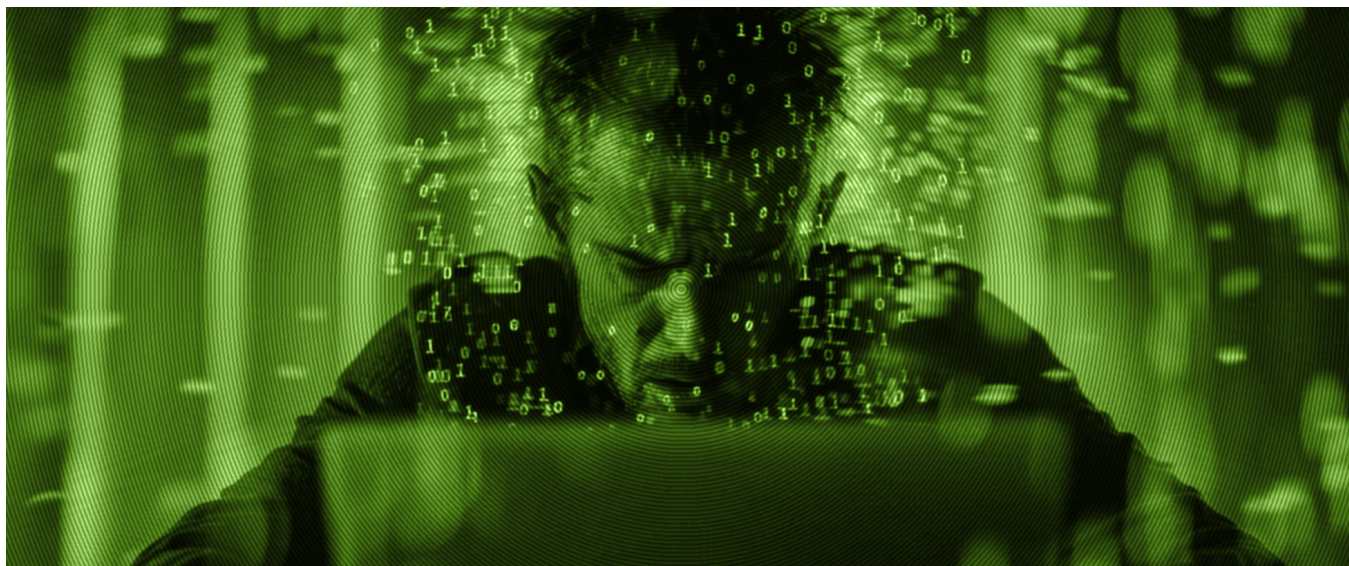
That said, the transition to version 4.0 isn't as daunting as it might seem, especially if you've already conducted a gap analysis and feel prepared. Many organizations have successfully implemented and validated their compliance with version 4.0. If you believe you can complete the transition and are comfortable with the requirements, moving to version 4.0 now is a viable option.

Ultimately, the decision should be based on your organization's readiness and commitment to security. If you want to demonstrate a proactive approach to security and feel confident about version 4.0, then migrating to the latest version is a good move.

What are two strategies to seamlessly transition to PCI DSS 4.0?

The first strategy is to ensure thorough planning and gap analysis while actively engaging with your Qualified Security Assessor (QSA). If you're undergoing a validation, early communication with your QSA, particularly concerning new requirements and the customized approach, is crucial. This proactive engagement helps clarify expectations and streamline the transition process. The council has provided extensive guidance and support to facilitate this move, addressing how criminals attack in the modern world.

The second strategy is to focus on getting the basics right. This involves a clear understanding of your environment, including what you have and how you use it. Collaborating closely with your internal security team and QSA team will help in identifying and addressing any gaps. By aligning your efforts and maintaining open communication, you can achieve compliance with PCI DSS 4.0, ensuring continued robust security.





Dawood Behbehani

AGM InfoSec – Privacy & Anti-Fraud,
Kuwait International Bank

As a member of the banking sector, how has the flexibility of PCI DSS 4.0 made it easier for you to meet your objectives? What advice would you give other organisations looking to implement a customized approach?

The new PCI DSS has introduced significant security countermeasures designed to help organizations secure their environments effectively. The customized approach, in particular, has been very beneficial for us. It allows us to comply with PCI DSS requirements while adopting innovative technologies.

For instance, our advanced machine learning solutions for fraud management didn't fit neatly into the defined approach requirements. Systems with machine learning capabilities require processing and storing large amounts of transaction data, which the defined approach couldn't

adequately support. The flexibility of the customized approach has been crucial for integrating these advanced technologies.

We have a robust and comprehensive risk assessment process that helps us understand and manage the risks associated with cardholder data. By working closely with our Qualified Security Assessor (QSA), we ensure that our customized approach is acceptable and that the necessary testing procedures are appropriate for our specific implementation.


My advice to other organizations is to engage with their QSA as early as possible. This early engagement can greatly facilitate the process of developing and implementing a customized approach, ensuring it meets PCI DSS requirements while addressing specific needs and technologies.

With targeted risk analysis becoming crucial, how did your organization effectively conduct TRA considering the extensive scope and multiple requirements involved?

Implementing targeted risk analysis requires a thorough understanding of the organization's scope under the PCI DSS. At our bank, we initiated this process by conducting a comprehensive workshop that brought together key stakeholders from business, IT, and information security teams. This collaborative approach helped us pinpoint unique risks specific to our operations.

Once these risks were identified, we implemented appropriate controls to mitigate them, often opting for solutions that provided equivalent or superior protection. We also integrated various technologies and processes that allowed us to regularly monitor and review the effectiveness of these controls, ensuring continuous protection based on the identified risks.

Auditors typically look for two key elements in the TRA process. The first is proper documentation that provides a clear trail of how risks were identified, assessed, and mitigated. The second is a justification of the frequency of activities, as pointed out by Jeremy. This documentation should clearly demonstrate how the chosen frequency addresses the entity's specific risks, ensuring that the organization's approach is both effective and compliant with PCI DSS requirements.



How can organizations achieve API and application security, and why is application-level security so important?

The importance of application-level security has been underscored by various lessons learned and breach cases globally. Often, user interfaces (UIs) or the applications themselves consume APIs that are inadequately secured. A common issue is that these APIs are over-permissioned, meaning they return more data than necessary, or they contain flawed authorization logic.

At our institution, we have tackled this challenge by integrating security earlier in the development process, a strategy known as 'shifting security to the left.' We've adopted agile methodologies and embraced the OWASP API top 10, which outlines the most critical security risks to web applications. This approach not only enhances our API and application security but also aligns with PCI DSS expectations on handling cardholder information.

Furthermore, we have emphasized end-user awareness by educating our teams on secure coding practices. This education is crucial because it helps individuals understand the nuances of security and the expectations of regulatory standards like PCI DSS.

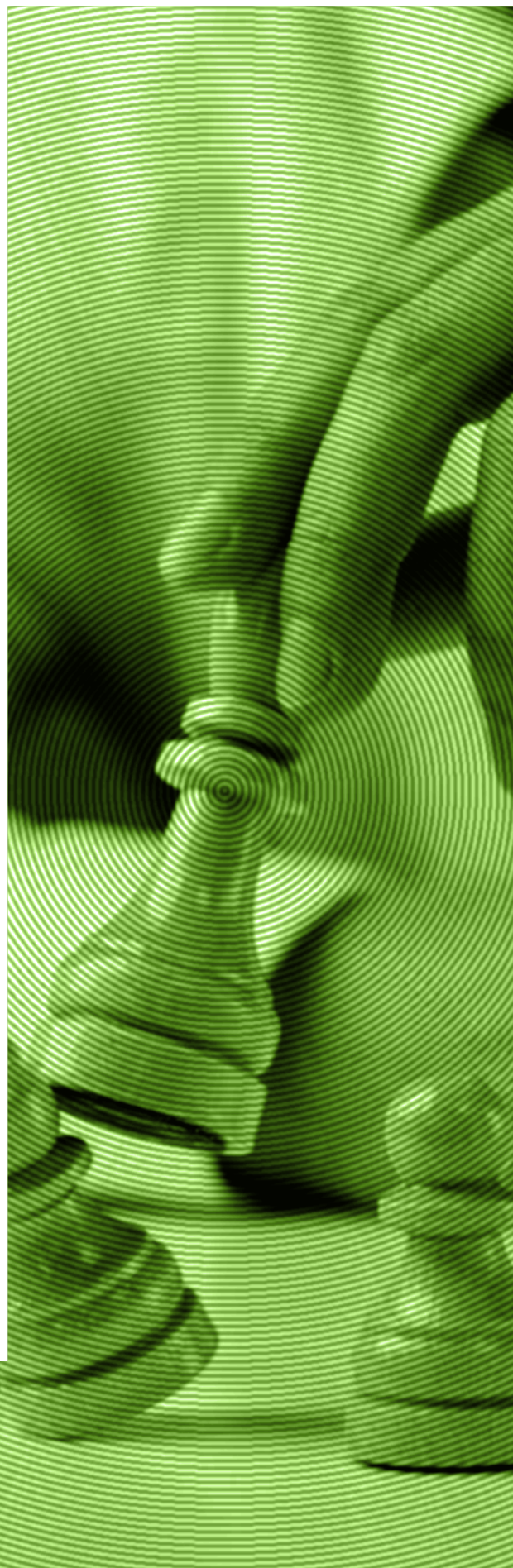
To continuously assess our security posture, we utilize tools that perform breach attack simulations. These tools regularly evaluate the security controls we have in place against emerging attacks, ensuring that our defenses remain robust and can thwart potential security breaches. This continuous assessment is vital in maintaining effective security measures at the application level.

As an implementer, how easy is it for organizations to change application and service level accounts? What are the critical steps and strategies to ensure the intent and objective of this requirement are met?

The primary challenge with access management is that accounts are often over-permissioned. This means that accounts can retrieve more data than necessary, which is a significant security risk. Attackers exploit these excessive permissions, and many accounts do not adhere to the principle of least privilege. Additionally, there is often no proper inventory of accounts, exacerbating the issue.

To address this, organizations should adopt privileged access management and endpoint access management solutions. Proper identity access management is crucial, as well as key management solutions to securely handle keys generated within the environment.

Changing application and service level accounts is not easy and requires careful planning. The complexity of the shift needs to be assessed, and a firm action plan must be in place. This plan should outline the steps necessary to achieve the intended objectives, ensuring that the organization meets the security requirements while minimizing disruption. By following these strategies, organizations can better manage permissions and secure their systems against unauthorized access.





● **Sam
Butler**

CISO, PayU, UK

Considering the customized approach in PCI DSS 4.0, what strategies can organizations adopt, especially in e-commerce or online payment security?

When using the customized approach, it's crucial to ensure that controls are prepared and evaluated, with a particular focus on risk assessment before the assessment itself. It's important not to use the customized approach as a compensatory measure for a lack of control. Instead, organizations should implement controls upfront, ensuring they are well understood and evaluated through targeted risk assessments.

From the perspective of targeted risk analysis, what strategies should organizations adopt to enhance their effectiveness?

Targeted risk analysis offers significant advantages by placing the security controls within the context of real-world threats, rather than theoretical risks. This approach not only helps validate the controls' effectiveness against actual threats but also provides a practical framework for continuous improvement. It allows organizations to prove to Qualified Security Assessors (QSAs) and other stakeholders that the security measures are not only in place but are robust and effective in the context of the specific threats they face.

Additionally, targeted risk analysis serves as a platform for identifying areas that require further enhancement. By focusing on the practical and real-world applicability of controls, organizations can ensure they are meeting the specific requirements of PCI DSS while also adapting to the evolving landscape of cyber threats. This approach ensures that the security measures are not just compliant but are truly effective and tailored to the organization's unique environment.

How important are payment page integrity checks for web pages related to payment information, and how can these checks be effectively implemented within an organization?

Payment page integrity checks are crucial for maintaining the security of web pages that handle payment information. These checks ensure that the payment pages operate as intended and are free from vulnerabilities that could be exploited by malicious actors. Implementing these checks requires good governance, a thorough understanding of how the pages are designed and operate, and robust hygiene practices.

In terms of implementation, it's essential to utilize tools that can automate the lifecycle management of these pages. Key strategies include rigorous testing and immediate remediation of any issues identified. Issues need to be addressed quickly and efficiently, within a reasonable timeframe to prevent exploitation. The focus should be on identifying and remedying vulnerabilities in the most urgent manner possible.

What additional strategies can you provide to ensure that the control of managing application and service level accounts is met in the easiest and most effective way?

Addressing the management of application and service level accounts is indeed a complex problem, especially if there are many legacy accounts that haven't been well managed. The first step is to understand the organizational perspective before implementing any technical changes. It's crucial to grasp the real role-based access requirements from a use case perspective rather than immediately focusing on tools and technology.

Organizations need to rethink and redesign access management as a concept. This involves significant effort to align with industry best practices, but it's necessary for reducing risks. The redesign should include a thorough understanding of who needs access to what and why, ensuring that permissions are tightly controlled and only granted based on actual requirements.

Additionally, organizations should not underestimate the effort required to redesign, rebuild, and reorganize their access management practices. By aligning with the real-world practices outlined by PCI DSS, organizations can significantly mitigate risks and enhance their overall security posture.

What are two essential strategies that organizations can consider for a seamless transition from unsupported versions of PCI DSS to version 4.0?

The first essential strategy is to thoroughly understand your environment, services, asset inventory, and their interdependencies. It's crucial to go back to basics and fully comprehend the environment you are responsible for securing. This foundational understanding helps in identifying and addressing specific areas that need attention during the transition to PCI DSS 4.0.

The second strategy is to cultivate a strong risk culture within the organization. This involves ensuring that decisions are made with a clear understanding of the associated risks and are supported by executives and stakeholders. Validating these decisions based on comprehensive risk assessments is crucial for maintaining continuous compliance and upholding good security practices. A robust risk culture helps in making informed decisions that align with the organization's security objectives and compliance requirements.

03

**SISA
Perspective**



From Legacy Systems to Modern Compliance: Adapting to PCI DSS 4.0

The Payment Card Industry Data Security Standard (PCI DSS) remains the gold standard for protecting sensitive cardholder data. However, the updated PCI DSS 4.0 version presents a significant challenge for organizations grappling with legacy systems. These outdated infrastructures can hinder compliance efforts and leave organizations vulnerable to modern cyber threats. Organizations must navigate several hurdles during the transition from legacy systems to PCI DSS 4.0 compliance.

Legacy systems often feature over-permissioned accounts, outdated security measures, and compatibility issues with new technologies. Overcoming these challenges requires a thorough risk assessment, strategic integration of new technologies, and a shift towards continuous compliance practices. Establishing a culture of security and risk management is essential to ensure long-term protection of sensitive cardholder data. This article explores the hurdles organizations face during the transition from legacy systems to PCI DSS 4.0 compliance, and the strategies for overcoming these challenges through effective risk management.



Challenges of Transitioning Legacy Systems

Legacy systems often lack the security features and flexibility demanded by PCI DSS 4.0. Here are some key challenges organizations encounter during the transition:



Over-permissioned Accounts

Legacy systems frequently struggle with granular access controls, leading to accounts with excessive permissions. This creates a larger attack surface for malicious actors who exploit these privileges to access and exfiltrate sensitive cardholder data.



Integration Difficulties

Integrating new security solutions with legacy systems can be complex and time-consuming. Patching and updates for older systems pose additional challenges, potentially disrupting critical business operations.



Limited Visibility and Control

Legacy systems may lack the centralized logging and monitoring capabilities essential for identifying and responding to security threats. This limited visibility makes it difficult to demonstrate compliance with the continuous monitoring requirements of PCI DSS 4.0.

Strategies for Adapting to PCI DSS 4.0

Despite these challenges, transitioning to PCI DSS 4.0 compliance with legacy systems is achievable. Here's how organizations can navigate this process:



Prioritize Access Control

Implement a least privilege principle, granting users only the minimum permissions necessary to perform their tasks. Utilize privileged access management (PAM) solutions to control and monitor privileged accounts. Conduct regular reviews and audits to identify and revoke excess permissions.



Embrace New Technologies

While complete system overhauls may not be feasible, consider integrating newer security solutions with legacy systems. Cloud-based security tools and containerization technologies can offer enhanced protection without requiring significant changes to core infrastructure.



Leverage the Customized Approach

PCI DSS 4.0 introduces the "customized approach," allowing organizations to demonstrate compliance by implementing alternative controls that achieve the same security objectives as the defined requirements. This flexibility can be invaluable when dealing with limitations imposed by legacy systems. However, close collaboration with a Qualified Security Assessor (QSA) is crucial to ensure the proposed controls are adequate.

Building a Culture of Continuous Compliance

Effective PCI DSS 4.0 compliance doesn't end with achieving initial validation. A continuous risk management approach is essential for maintaining a secure environment. Here are key steps to fostering this culture:



Regular Risk Assessments

Conduct regular risk assessments to identify and prioritize potential security threats. Analyze vulnerabilities within legacy systems and tailor security controls to address them.



Invest in Employee Training

Educate employees on PCI DSS requirements and best practices for handling cardholder data. Role-based training programs can raise awareness and equip employees to identify and report suspicious activities.



Automation and Monitoring

Leverage automation tools to streamline security tasks like vulnerability scanning and log analysis. Continuous monitoring of systems and network activity facilitates early detection and response to security incidents.

Conclusion

Transitioning to compliance with PCI DSS 4.0 while managing legacy systems requires a strategic approach. Organizations must prioritize access control, embrace new technologies where feasible, and leverage the customized approach. By cultivating a culture of continuous compliance through risk management, employee training, and automation, organizations can bridge the gap between legacy systems and modern security standards. This not only ensures PCI DSS compliance but also fosters a more secure environment for protecting sensitive cardholder data in the digital age.



About SISA

SISA is a global forensics-driven cybersecurity solutions company, trusted by leading organizations for securing their businesses with robust preventive, detective, and corrective cybersecurity solutions. Our problem-first, human-centric approach helps businesses strengthen their cybersecurity posture. We apply the power of forensic intelligence and advanced technology to offer true security to 2,000+ customers in 40+ countries.

SISA is one of the leading global forensic investigators for the payments industry.

Compliance	Security Testing	Cyber Resilience	Data Protection & Governance	SISA Institute
Payment Data Security <ul style="list-style-type: none"> • PCI DSS • PCI PIN • PCI 3DS • PCI P2PE • PCI S3 • PCI S-SLC • PCI CP (Card Production) • Facilitated PCI SAQ • Quarterly Health Check-ups • Central Bank Compliance • SWIFT Strategy and Risk <ul style="list-style-type: none"> • CCPA • GDPR • HIPAA • ISO • NIST • SOC 1 • SOC 2 • Cloud Security • HITRUST Unified Compliance Management Managed Compliance	Application Security <ul style="list-style-type: none"> • Application Penetration Testing • CREST/CERT-in Approved Security Testing • API Security Testing • Secure Code Review Network Security <ul style="list-style-type: none"> • Vulnerability Assessment • Penetration Testing • Configuration Review • Firewall Rule Review • PCI ASV Scan Phishing Simulation Red Teaming Exercise Hardware and IoT Security Testing <ul style="list-style-type: none"> • Firmware Security Testing • Hardware/Embedded Security Testing • IoT Network Security Testing • IoT/Embedded Application and Management Layer Security Testing 	Managed Extended Detection and Response Solution - SISA ProACT <ul style="list-style-type: none"> • Monitoring • Attack Simulation • Use-case Factory • Advanced Threat Hunting Digital Forensics and Incident Response <ul style="list-style-type: none"> • Incident Response / Compromise Assessment Services • Forensic Readiness Audit • Forensic and Incident Response Retainer Service • Payment Forensics Investigation • Internal Forensics Investigation • Ransomware Simulation 	Data Discovery and Classification Tool - SISA Radar <ul style="list-style-type: none"> • PCI/PII/PHI Data Discovery • Data Classification in Endpoint (Windows, Linux) • Data Classification in 0365, Metadata • Dynamic Masking, Redact, Truncation • Integration to DRM, DLP, SIEM • IDeployment and Implementation Support • Product support • Demos and PoC in the client's environment • Training and KT Data Protection and Governance Managed & Shared Services <ul style="list-style-type: none"> • Data Security Assessment & Recommendations • Consultation & Data Risk Assessment support 	Payment Data Security Implementation Training and Certifications <ul style="list-style-type: none"> • CPISI • CPISI Advanced • CPISI-D (Developers) Certification Program in Cybersecurity for AI <ul style="list-style-type: none"> • CSPAI Cybersecurity Awareness Forensic Learning Sessions for Senior Management

USA | Canada | UK | Bahrain | Saudi Arabia | UAE | Qatar | India | Singapore | Malaysia | Australia

To learn more about SISA's offerings visit us at www.sisainfosec.com or
Contact your SISA sales representative at contact@sisainfosec.com