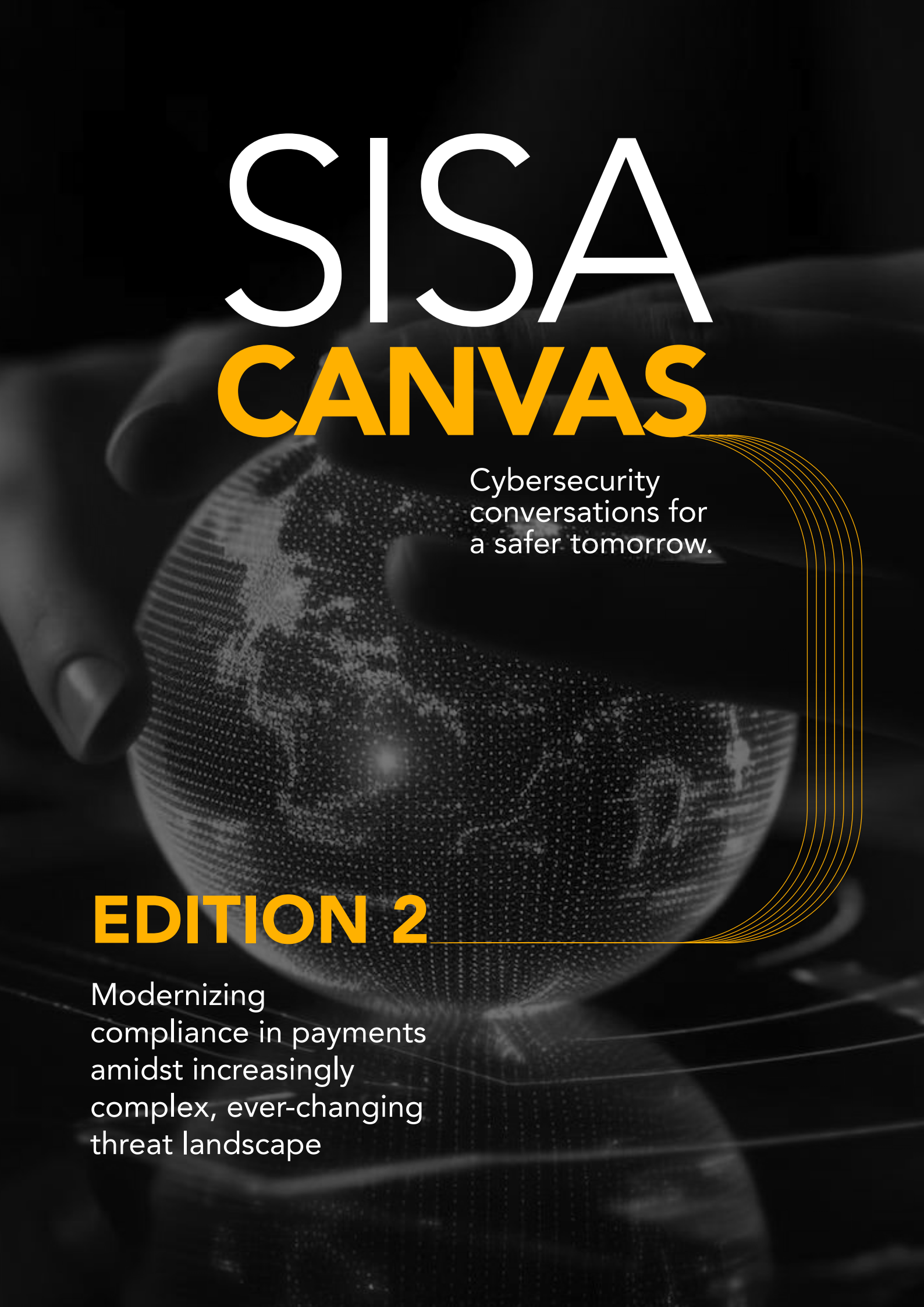

SISA CANVAS

Cybersecurity conversations for a safer tomorrow.

EDITION 2

Modernizing compliance in payments amidst increasingly complex, ever-changing threat landscape

Table of Contents

01 From the CEO's desk

Dharshan Shanthamurthy – CEO & Founder, SISA

02 Conversations with Industry Experts

- Nitin Bhatnagar – Regional Director India and South Asia, PCI Security Standards Council
- Dr. Rebecca Wynn – Chief Cybersecurity Strategist, Global CISO, Privacy and Risk Officer, Author, Keynote Speaker, Consultant
- Pravin Kumar – CISO, Wibmo - a PayU company
- Layeequr Rahman – Asst. Vice President - InfoSec Governance Risk & Compliance, [24]7.ai

03 Executive Viewpoint

Sachin Sawant – VP, Compliance and Testing, SISA

04 SISA Perspective

The role of AI in improving compliance and audit processes in the payments space

From the CEO's desk

Dharshan Shanthamurthy

CEO & Founder, SISA

Dharshan Shanthamurthy is the founder and CEO of SISA. With more than two decades of experience, he is missioned to protect businesses from cyber-criminals. He works closely with CXO's of businesses to draw their cybersecurity strategy and improve their security posture. A pioneer in the payment security space, he is the first Payment Security Assessor in Asia and a core Payment Forensic Investigator.

Step into the world of the digital age, where technological advancements have revolutionized the way we handle our finances. It's an era filled with endless possibilities and incredible convenience. However, amidst the marvels of this new era, a lurking danger awaits—cyber threats, more cunning and sophisticated than ever before.

Picture this: cybercriminals, equipped with advanced techniques and exploiting vulnerabilities in payment systems, are prowling the virtual realm, searching for their next target. In this high-stakes game, safeguarding sensitive payment data has become the holy grail for businesses of all sizes.

Traditionally, compliance with industry regulations and standards has been the bedrock of payment security. Yet, as the threat landscape continues to evolve, it's clear that the old ways of doing things are no longer enough. We stand at a crossroads, faced with the urgent need to modernize payment compliance.

This is a call to embark on an exhilarating journey—one that involves embracing innovative strategies, harnessing cutting-edge technologies, and fostering a culture of continual improvement.

Imagine a future where businesses are armed with state-of-the-art tools that outsmart even the most cunning cybercriminals. A future where organizations proactively anticipate and counter emerging threats, rather than reactively scrambling to recover from an attack.

In this journey towards modernizing payment compliance, we explore uncharted territories, where creativity and ingenuity flourish. We employ groundbreaking technologies like artificial intelligence, machine learning, and blockchain to fortify our defenses. We leverage the power of data analytics to identify patterns, anomalies, and potential breaches before they can wreak havoc.

But it's not just about technology. It's also about fostering a culture that champions security at every level. We educate and empower employees, transforming them into the first line of defense against cyber threats. We encourage a mindset of constant vigilance and proactive risk management, where everyone becomes a guardian of payment data.

On the regulatory front, we see the continuous evolution of compliance frameworks and norms. Regulatory bodies recognize the need to adapt to the ever-changing threat landscape and are enacting increasingly stringent guidelines to protect payment systems. Simultaneously, organizations are becoming more cognizant of the necessity of robust compliance and security practices. Businesses are becoming more aware of the possible impact of cyber catastrophes on their brand and customer trust as high-profile data breaches continue to make headlines.

SISA, as a staunch believer in true security, stands prepared to aid organizations in adapting to these transformative developments. Our goal is to ensure their compliance with ever-evolving regulations while fortifying their security posture. We are dedicated to crafting state-of-the-art solutions driven by forensic intelligence, offering enterprises a comprehensive platform to seamlessly oversee every facet of the data lifecycle process.

Conversations with Industry Experts

Nitin Bhatnagar

Regional Director India and South Asia, PCI Security Standards Council

Nitin leads the PCI Council's efforts in increasing adoption and awareness of the PCI Security Standards in India and South Asia. In this role, Mr. Bhatnagar works closely with the PCI Council Management Team, Payment Brands, Assessors Community, Participating Organization, Government entities and Regulators. Mr. Bhatnagar is an innovative thinker, speaker, television personality, and technical writer and has been often quoted in cybersecurity news stories including the BBC, ET Now, CNBC TV 18, Reuters, Economic Times, and Times of India.

PCI DSS 4.0: From Defined to Customized Approach – A Paradigm Shift in Payment Security

In light of the market's dynamic technological landscape, including the cloud, the Internet of Things (IoT), and new payment methods, how does PCI DSS 4.0 adapt to these changes and ensure the security of payment data?

The requirements in PCI DSS have always been based on fundamental security principles that are applicable in all kinds of environments, regardless of technology. Even if a particular technology is not mentioned in the standard, the security requirement's intent still holds true. The latest iteration of PCI DSS has incorporated objective statements that offer improved support for diverse technologies, including cloud environments. Moreover, the requirements have been restructured to underscore their wide-ranging relevance across all types of technology. In order to promote security, PCI DSS 4.0 adopts a tailored approach that accommodates a range of evolving payment environments, technologies, and methodologies. This customization aims to address the specific needs and challenges of different contexts while ensuring robust security measures are implemented.

The customized approach offers greater flexibility to entities when they use various technologies or processes to fulfill the objective of the requirement. This provides a clear understanding of the necessary actions while allowing greater flexibility to help organizations attain their desired security outcome. The PCI DSS requirements, for instance, now include a section that specifically mentions cloud components. Appendix A1, which was formerly for Shared Hosting Providers, has also been revised. Cloud service providers are now included in the category of multi-tenant service providers.

These service providers must now assist their clients with penetration testing, per a new requirement. Since many of the frequencies as well as the new standards are risk driven; focused risk assessment for PCI scope where you are taking the critical assets like the card data, sensitive authentication data, or card numbers, is going to play a very crucial role.

How has PCI DSS 4.0 evolved on authentication?

Many of the changes to authentication requirements have been driven by industry feedback and the changing threat landscape. A new requirement that MFA be implemented for all CDE access will go into effect on March 31, 2025. The updated standard also clarifies that MFA is required for both CDE access and remote access originating outside the entity's CDE. Applying it to only one type of access does not eliminate the need to apply for another MFA.

The second revision concerns passwords or passphrases. The password length has been increased from seven to twelve characters in response to feedback that seven characters are no longer sufficient for modern computing power. The limit of twelve characters will be implemented on March 31, 2025. Until then, entities must use seven characters in accordance with PCI DSS v3.2.1. We have retained the requirement to change passwords every 90 days because for some entities, passwords are the only form of protection they have, and changing them on a regular basis can prevent previously breached walls from being reused. However, the requirements to change passwords will only apply to systems that do not have

MFAs, such as those in scope but not in the CDE. The password change requirements for systems protected with MFA can be marked as NA.

Another evolved requirement is for group, shared, generic accounts. The use of these accounts was prohibited in version 3.2.1. This requirement has been modified in the new version so that entities can use them in exceptional circumstances such as limited timeframe justification, user identity approval/confirmation, and actions attributable to individuals.

The updated standards reflect industry feedback and the evolving threat landscape, emphasizing the implementation of multi-factor authentication (MFA) for all CDE and remote access, increasing password length to twelve characters, and allowing the use of group accounts in exceptional circumstances.

What does PCI DSS 4.0's new customized approach entail? Which types of organizations are best suited for adopting a customized approach, a defined approach, or a hybrid combination of both methodologies to meet their specific security needs and requirements?

In addition to the defined approach for meeting PCI DSS requirements, the customized approach is a new validation option. The defined approach adheres to the traditional PCI DSS requirements and testing procedures to ensure compliance – the Qualified Security Assessor (QSA) goes onsite and follows the standard policies and procedures before the implementation takes place. The customized approach on the other hand, provides flexibility to organizations to achieve a requirement's security objective in a way that differs from the defined approach. To elaborate, the customized approach requires entities to identify controls and then implement them to achieve the stated customized approach objective. They must, however, provide a clear demonstration that the payment data is secure. The customized approach empowers organizations to leverage alternative security controls for advancements in security technology and methodologies, offering greater flexibility in applying the requirements to diverse environments. It is important to note that a customized approach is not a replacement for compensatory controls. While compensatory controls remain in place, any organization opting for a customized approach cannot use compensatory controls.

The customized approach is intended for organizations that have robust security processes and risk management practices. It includes, but is not limited to, a dedicated management department or an organization-wide risk management approach. The defined approach assists entities that have controls in place that meet the stated PCI requirement.

This approach may also suit entities that want more guidance on how to meet security objectives, such as those new to information security or PCI DSS. They can eventually choose the customized approach as they grow and advance to the next level by having a dedicated risk management department.

The customized approach empowers entities with robust security processes and risk management practices to leverage alternative security controls while still ensuring the security of payment data.

Most PCI requirements can be met using either approach. However, several requirements lack a stated customized approach objective, so the option is inapplicable there. Entities have the flexibility to employ a combination of the defined and customized approaches within their environments, utilizing the defined approach to fulfill certain requirements while leveraging the customized approach to address others more effectively. As a result, a PCI DSS assessment can incorporate both defined and customized approaches. However, it must be designed in consensus with a QSA. It is crucial to highlight that when businesses opt for the customized approach, they should be aware that the same Qualified Security Assessor (QSA) who provides guidance cannot certify their organization for PCI DSS 4.0. This is due to the heightened emphasis on accountability and responsibility for maintaining all controls to meet the requirements, driven by the rise in security breaches, particularly within the payments industry.

Dr. Rebecca Wynn

Chief Cybersecurity Strategist, Global CISO, Privacy and Risk Officer, Author, Keynote Speaker, Consultant

Dr. Rebecca Wynn - Named a Top 100 Women in Technology 2021 - IBM; Top Inspirational Women in Technology 2021; Business Role Model of the Year 2018; Cybersecurity Professional of the Year 2017 - Cybersecurity Excellence Awards; podcast host; author. She is lauded as a "game-changer who is ten steps ahead in developing and enforcing cybersecurity and privacy best practices and policies." She is a "big picture" thinker who has over 20 years of experience in Information Security, Assurance & Technology.

From Version 3.2.1 to 4.0: The Game-changing Innovations of PCI DSS

In your view, what was the driving force behind the introduction of PCI DSS version 4.0? Additionally, what is your estimation of the average timeframe that organizations will require to successfully adapt, implement, and navigate through the transformation process?

One of the main causes for the urgent need for the new PCI DSS version is new and emerging threats. We need to realize that we are constantly engaged in a cyberwar and need to step up our game. Therefore, it is important to incorporate security, compliance, and privacy into your very fabric. PCI DSS is not the only regulation that is being upgraded. You will find improvements in other regulations as well, including NIST 800-53r5 and others. You will, therefore, notice some similarities among all those regulations. And businesses that are already compliant with them are beginning to implement some positive changes for PCI DSS 4.0.

The second thing to notice is that, if businesses have cybersecurity insurance, they will find that it is already helping them meet some of these requirements. Therefore, organizations must eliminate any and all ambiguity, be able to deal with cyber threats, and persuade the team that this must be a constant part of their culture and not just a checkbox that needs to be ticked.

Considering that the timelines are fast approaching, they must begin right away. The year 2024 will soon be upon us, and as I constantly remind people, you never know what global catastrophe may strike, diverting your attention and resources to other areas. Businesses need to get the strategic plan in place right away so that they can set up budgets and personnel.

It is also important to note that by March 31, 2024, there are a few best practices that everyone should have in place. Although the new PCI requirements will not be enforced until March 31, 2025, their legal contracts may require them to have those best practices in place.

When it comes to technical requirements, PCI DSS has always been at the forefront of the industry. According to you, what are some of the most significant technical changes to the PCI DSS 4.0 requirements?

There have been numerous changes in the new standards, but some of them are quite noteworthy for businesses. One of them is about full disk encryption. We have known for a long time that full disk encryption is no longer a reliable safety net. So, if companies are still using full disk encryption and not looking at other ways to do cryptology, they will have to invest significant time and resources into assessing their processes to align with the new standards.

Multi-factor Authentication (MFA) emerges as another critical factor. With the increased utilization of remote desktop software, relying solely on an organization's authentication server becomes ineffective. Consequently, businesses will need to engage a third-party service for authentication purposes. While certain organizations have already undergone this transition, they will now need to replicate it within their card environment, potentially necessitating the procurement of additional licenses and the recruitment of more staff members. Hence, this becomes another domain where a substantial investment is required.

Regarding log review, it is common for businesses to already possess a Security Information and Event Management (SIEM) system, although some rely on alternative methods. However, the new requirement for a SIEM or a next-generation SIEM represents a substantial investment for numerous companies. Additionally, they must address the critical question of who will oversee and monitor the influx of alerts generated by the system. This necessitates either enlisting the assistance of a third-party vendor or hiring and training internal employees to fulfill this role effectively.
Vulnerability scans present another significant area of consideration. Businesses now need to distinguish between authenticated and unauthenticated scans, potentially requiring modifications to their current software, systems, or platforms if they are not supported. Moreover, they must carefully plan how they will incorporate additional equipment and provide training for personnel to effectively manage and monitor these authentications. This highlights the need for careful assessment and allocation of resources in order to fulfill the new requirements.

PCI DSS 4.0 introduces a substantial change by mandating that third-party service providers must now support penetration testing (pen testing). Consequently, businesses must carefully review and update existing contracts with such providers. Monitoring service providers to ensure compliance with PCI standards becomes imperative. If a service provider fails to meet these new requirements, businesses may have to consider switching to alternative providers capable of meeting the revised standards. This underscores the need for ongoing vigilance and assessment of third-party relationships to maintain compliance.
These are a few of the factors that are in play, so organizations need to consider their budget, personnel, working with the company, and incorporating this into their products and rollouts.

In the new standards, businesses face notable changes, such as the need to move beyond full disk encryption, invest in multi-factor authentication, acquire SIEM or next-generation SIEM systems, manage authenticated and unauthenticated vulnerability scans, and ensure compliance of third-party service providers.

What is your opinion on the introduction of the customized approach to the PCI DSS standards, which has been eagerly anticipated by many?

Overall, I believe it can be risky. I say this because some businesses may consider it to be a loophole through which they can avoid complying with requirements. Implementing a customized approach is better suited for well-established or larger organizations that are at the forefront of technology adoption and employ diverse technologies or a blend thereof to meet control objectives. This gives them the freedom to do that, but it is also a more difficult route. Utilizing the templates provided, they will need to conduct additional assessments and documentation for customized approach.

There is also a lengthy decision tree. It is possible to slightly customize the approach by basing some of it on the standard metrics, but businesses must be able to methodically justify that. However, organizations that are small or medium-sized must also not consider it an easy method because it would be a heavier burden.

New technologies and methods of doing things are constantly emerging as we talk about moving to 2025 or 2026, primarily because we are constantly engaged in a cyberwar. Businesses can show how they protect cardholder data and adhere to those controls by using a customized approach that allows them to grow and expand. However, if organizations believe it will serve as their "get out of jail free" card, that is not what it means.

Pravin Kumar

CISO, Wibmo - a PayU company

Pravin has spent most of his career in technology, audit, DevSecOps, GRC, Cyber, Data Governance and Privacy. His expertise includes developing, implementing, maintaining, and overseeing enforcement of information security policies, procedures and standards based on industry-standard best practices. He has acquired certifications like CISSP, TOGAF 9, PMP, CISA, CRISC, CISM, CGEIT, ITIL and many more.

Beyond Compliance: A CISO's Take on Addressing Top Payment Application Security Concerns

How crucial is application security in ensuring the security of payment systems, considering the finding from SISA's Top 5 Forensics-driven Learnings report that attributes compromised organizations to the absence of robust application security?

In the payments sector, CISOs, security managers, and risk managers must exercise heightened caution when it comes to application security. Working with sensitive data, such as credit card or payment information, adds an additional layer of responsibility. The security of payment applications carries a weightier burden compared to applications in other industries. To establish a controlled environment for all applications, it is essential to approach the planning process with careful consideration and sensitivity to the business and data involved.

For instance, at Wibmo, we engage in product marketing and sell products and services to our customers, the majority of whom are banks. First off, dealing with banking clients exposes us to a heavy dose of complex compliance regulations. When compared to other industry applications, this is another distinction. Secondly, the nature of the data we deal with—personally identifiable information (PII), credit card numbers, payment transactions, etc.—increases responsibility. Thirdly, we use many APIs and integrate many systems.

Therefore, while designing the controls, businesses should be aware of their footprint and the full landscape of their threat surface. Together, these three factors set application security in the payments industry apart from other environments for application-related security control. No matter which framework we use, the fundamentals remain the same. The primary components must all be present.

I put this into practice by treating all applications equally, including my critical set of applications. I firmly believe that control measures should be applied consistently to every application and infrastructure component. While certain applications may demand heightened attention, the standard control framework serves as the foundation for all. Any additional compliance requirements or industry standards are layered on top of this comprehensive approach.

Complex compliance regulations, the responsibility of handling sensitive data, and the challenge of integrating multiple systems, set application security in the payments industry apart, emphasizing the importance of comprehensive controls and fundamental components for effective protection.

As one of the biggest players in the fintech sector, what are your top three primary security concerns?

One of my top three concerns as a prominent player in the fintech sector is having a comprehensive understanding of our footprint. This encompasses key questions such as: Do we have a clear inventory of our APIs? Are we aware of all the infrared equipment supporting our applications? Do we have visibility into who has access to these resources and where they are located? Therefore, contextual awareness of our application ecosystem is a significant concern for me.

The second concern revolves around the challenge of finding and recruiting individuals with genuine talent who possess a deep understanding of application security. While many candidates may hold numerous certifications, it is rare to find individuals who truly comprehend application architecture, coding practices, threat landscapes, mitigation strategies, as well as DevOps and website security. My advice to businesses is to prioritize application security or API security if they genuinely aim to progress in cybersecurity.

Application security or API security holds immense importance as it represents the future of secure software development and data protection.

The third main concern revolves around the transition from on-premises to a cloud environment. While migrating to the cloud is a prevalent industry trend, it comes with its own set of challenges. From my discussions with CISOs and security experts, it is clear that many businesses are eager to embrace the cloud. However, it is crucial to acknowledge and address the multiple challenges that arise during this transition.

To assess the residual risk and determine their standing, I advise businesses to diligently plan and create a cloud security risk inventory. The risks associated with cloud application security, including identity and access management, are of utmost concern to me.

In my view, these three risks hold significant importance in the fintech domain. However, at a broader level, there are additional risks that organizations must consider. One such risk is the supply chain, exemplified by incidents like the log4j vulnerability, which highlight the potential dangers of relying on third-party components. Additionally, malicious actors consistently exploit vulnerabilities outlined by the Open Web Application Security Project (OWASP) that organizations often overlook. These are among the critical risks that application security professionals must address.

How does your business effectively meet the overlapping controls across multiple regulations such as PCI, ISO, NIST, SOC, PCI SLC, and PA DSS, without succumbing to compliance fatigue?

On the application side, we have effectively addressed the challenge of overlapping controls across PCI, ISO, SOC, PCI SLC, and PA DSS through the implementation of a unified control framework (UCF) or integrated control framework. At Wibmo, we achieved approximately eight certifications within a year, which is likely a remarkable feat for any organization. The UCF approach, based on the 'test one, certify many' ideology, has been instrumental in our success. We have developed a clear understanding of the required controls and evidence for each compliance standard, allowing us to navigate through the certification processes efficiently.

In my opinion, it is crucial for a CISO to be aware of, or invest in, the development of a unified and integrated control framework. By combining these standards with your organization's specific legal and industry requirements, you can create a comprehensive, accurate, correct, and complete framework. This can be referred to as Risk Control Metrics (RCM), which encompasses your risks, compliance requirements, necessary controls, and assigned responsibilities. By documenting these in a consolidated sheet and assigning control ownership, you can efficiently manage and track them.

The Unified Control Framework (UCF) streamlines compliance efforts by consolidating multiple regulations, standards, and frameworks into a unified set of controls. It promotes efficiency, consistency, and effectiveness in compliance management, optimizing resources and reducing redundancy.

Taking a proactive approach to compliance management, such as implementing an integrated control framework like RCM, allows organizations to streamline their compliance efforts and mitigate the risk of compliance fatigue. It provides clarity, accountability, and a structured approach to meeting the requirements of multiple regulations while efficiently managing controls and responsibilities.

Layeequr Rahman

Asst. Vice President - InfoSec Governance Risk & Compliance, [24]7.ai

Passionate, self-motivated leader with Business-focused technology & service industry leader with 20+ years of management and leadership distinctions. Highly organized with a focus on simplicity, innovation, and global change management. Experience ranges from implementing Six Sigma to Corporate Governance, Risk Management, Continuous Compliance, Information Security, Security Incident Management, Business Continuity Management and Project Management for Global organizations

Strengthening Compliance with Data Discovery Tools and Proactive Incident Response

How does the utilization of a Data Discovery or card finding tool contribute to meeting compliance regulations, particularly PCI DSS 4.0, in the payments industry?

Data discovery has long been a part of PCI standards, and its inclusion in the standards is crucial. One of the largest or most significant risks that a business faces today is in terms of how and where its data is stored. Cardholder data is frequently stored as unidentified data points. Unintentional or inadvertent card data storage can be a primary source of any breach or incident. To mitigate these risks and prevent breaches, organizations need to establish procedures and mechanisms for discovering and securely deleting card data whenever it is no longer necessary or beyond a specific retention period. This emphasizes the significance of data discovery tools in helping businesses identify and manage potential sources of cardholder data exposure, ensuring compliance with PCI DSS 4.0 and protecting against data breaches.

To enhance data security, compliance, and system consistency, enterprises should expand their data discovery scope, conduct regular scans across platforms, and schedule them during non-peak hours to minimize operational impact

To begin, I would recommend that enterprises widen the scope of their data discovery to include the entire corporation rather than simply the cardholder data environment. Cardholder data is frequently discovered unexpectedly outside the CDE, in places where it is not supposed to be retained. Second, when data is scattered across various platforms, enterprises frequently feel that adopting preventative control technology is enough to secure their environment. However, depending on the versions of those specific technologies or the rules applied in them, some controls may not cover all databases, operating systems, mailboxes, and so on. Running discovery scans is critical for assuring data security, compliance, and system consistency. Finally, the timing of these scans is vital. Businesses must ensure that they run them during lean hours to avoid affecting production.

The updated version of PCI DSS, i.e., v 4.0, puts a great emphasis on log monitoring and incident response. What are the new requirements in the standards and what actions should organizations take to comply with them?

QSAs now evaluate incident response procedures regardless of breach occurrence, emphasizing the significance of well-defined plans, roles, processes, and timelines to meet audit requirements and maintain proactive security measures

The requirements in the standard entail establishing robust methods within enterprises to promptly detect risks, generate alerts, and address critical security control failures. The effectiveness of this process relies on the SIEM (Security Information and Event Management) tool utilized by organizations. Some SIEM tools offer pre-defined templates or algorithms that streamline and expedite these tasks, ensuring efficient compliance with the requirement. By implementing audit log automation with a suitable SIEM solution, enterprises can enhance their security posture and swiftly respond to potential threats and control failures. However, in other circumstances, security teams may be required to develop customized code or scripts, which would necessitate greater effort. This helps ensure that the log reviews are diligent and versatile.

Previously, Qualified Security Assessors (QSAs) focused on incident response only in the aftermath of a breach. However, under the new approach, QSAs will review incident response procedures irrespective of whether an actual breach occurred or if it was a suspected incident or false positive. The roles and responsibilities assigned during an event, along with the associated playbook, processes, and timelines, will carry significant weight in the assessment process.

It highlights the growing importance of having robust and well-defined incident response plans, regardless of the occurrence of a security incident, to meet the requirements of audits and maintain a proactive security stance.

What are the best practices that organizations must consider when transitioning to meet compliance with PCI DSS 4.0?

Procrastination, first and foremost, is not an option. PCI has given us ample time to become acquainted with the adjustments. If an organization has a strong team that can work together and conduct a gap analysis to determine where they stand, I would advise them to go with it; otherwise, seek assistance from a QSA. If they are renewing their PCI DSS 3.2.1 certification, they can begin working on a review in terms of 4.0 to see what components they need to improve.

The changes introduced in PCI DSS 4.0 can be broadly categorized into two areas: changes in methodology and changes in requirements. Methodological changes primarily involve documentation, roles, and responsibilities, which are relatively straightforward and should be considered as low-hanging fruit. Additionally, organizations must also pay attention to changes in security protocols and rules.

Another significant modification in PCI DSS 4.0 is the heightened focus on continuous compliance. This means businesses are required to periodically confirm the scope of their PCI DSS assessment. Depending on the infrastructure and chain management, organizations may need to conduct this assessment every six months or more frequently.

It is crucial for businesses to take stock of their entire ecosystem to ensure compliance with the evolving requirements.

In addition to meeting PCI DSS compliance, organizations must invest in new technologies and enhance risk maturity based on their specific needs. For instance, the new requirement for phishing attacks not only emphasizes specific technical controls but also necessitates comprehensive training for the team. I have noticed that it is common for organizations to focus solely on deploying technology, neglecting the importance of the "human firewall" in securing the business and achieving PCI DSS compliance. Businesses ought to look at not only meeting the PCI DSS standard, but also at how they want to ensure the overall security of their organization.

Executive Viewpoint

Sachin Sawant

VP, Compliance and Testing, SISA

Sachin is a highly accomplished professional with over 23 years of diverse experience in IT and Cybersecurity.
He presently oversees the Compliance and Testing Services business unit as Vice President at SISA. Sachin holds a number of prestigious certifications that demonstrate his expertise in payment security. Among other qualifications, he is a Payment Card Industry Qualified Security Assessor (PCI QSA), Certified Information Security Manager (CISM), and Certified Information Security Auditor (CISA). Throughout his career, Sachin has performed 100+ audits and assessments such as PCI DSS audits, Central Bank Regulatory Audits, and System Audits, for global payment enterprises including banks, payment aggregators, payment gateways, prepaid payment instruments, fintech solutions, tokenization platforms, and other service providers. He is well-versed in the industry's intricacies and stays abreast on the newest trends and best practices. Sachin's extensive cybersecurity experience and expertise enable him to solve the most complex issues and develop effective solutions for enterprises seeking robust security measures.

From CBDCs to Cryptocurrencies: Ensuring Compliance in the Brave New World of Payments

How do you see compliance and regulatory standards catching up with the breakneck pace of innovation & tech adoption in digital payments? Can we expect newer models beyond sandbox and light-touch regulation, that can balance out security and innovation?

Compliance and regulatory standards are critical in guaranteeing the safety, security, and stability of digital payments, especially as innovation and technology adoption grow at an accelerated pace. However, keeping up with the constantly evolving landscape of the digital payments industry can be challenging for regulatory bodies. To solve this, several regulatory entities have adopted a sandbox approach, which allows experimentation in a controlled environment while maintaining a certain level of regulatory oversight. This approach can be useful for testing new digital payment methods while simultaneously confirming that they meet regulatory standards.

However, as the industry evolves, we may see innovative models that go beyond the sandbox and light-touch regulation. A risk-based approach is one such model, in which regulatory requirements and control are proportionate to the level of risk posed by a certain digital payment model. This would enable a more focused regulatory strategy that would balance innovation and security. Another potential option would be to deploy technology-based solutions to enforce compliance and regulatory standards. Artificial intelligence (AI) and Machine Learning (ML), for example, can be used to detect suspicious transactions and prevent fraud while also ensuring regulatory compliance.

Overall, I believe that a collaborative approach to compliance and regulation is key to ensuring that the digital payments industry continues to innovate while maintaining a strong focus on security. By working together, regulatory bodies and industry stakeholders can develop frameworks that are both effective and practical, allowing for continued growth and innovation in the digital payments space.

As the industry evolves, innovative models that transcend sandbox environments and light-touch regulation may emerge, such as the risk-based approach, where regulatory requirements and controls are tailored to the level of risk associated with specific digital payment models.

Nations worldwide are witnessing the emergence of evolution in payment methods such as the growth of CBDC (Central Bank Digital Currencies), BNPL (Buy Now Pay Later) and Cryptocurrencies. How can organizations ensure security and compliance amidst such a transformation?

The emergence of new methods of payment uch as CBDC, BNPL, and cryptocurrencies can present enterprises with both opportunities and challenges. While these advances might improve financial transaction convenience, speed, and efficiency, they can also introduce new security and compliance issues that must be addressed.

To begin with, enterprises must monitor the changing regulatory landscape around payment methods such as CBDC and cryptocurrencies to ensure compliance with the relevant laws and regulations. To mitigate identified risks, businesses must invest in comprehensive security measures such as a multi-layered security architecture, data encryption, access controls, and real-time monitoring. Additionally, businesses should consult with experts and third-party partners to get new insights and leverage their expertise to ensure compliance and security. Furthermore, when partnering with payment providers or vendors, organizations must conduct extensive due diligence on their security and compliance processes. They should ensure that payment providers have adequate safeguards in place to prevent fraud and comply with applicable laws and regulations.

Another thing to keep in mind is that security and compliance are the responsibility of all stakeholders, not just the security team. Businesses should educate employees and customers on risks and best practices related to new payment methods. This includes training personnel on detecting and reporting fraudulent activity and educating customers on how to safeguard their personal and financial information.

In the pursuit of compliance and security, organizations should seek guidance from experts and third-party partners, harnessing their insights and expertise, while conducting thorough due diligence on payment providers to ensure robust safeguards against fraud and adherence to relevant laws and regulations.

Do you see a multipolar global order for payments compliance with regional/local standards driving the show or will it lean towards a major block/region and others following suit?

The trend toward multipolarity in global payments compliance appears to be gaining traction. Several causes are contributing to this trend, including the growing relevance of regional and local standards, the emergence of digital currencies and payment systems, and geopolitical shifts that are redefining global power dynamics.

In this context, it is likely that individual regions will continue to build their own payment compliance standards and systems to reflect their unique economic and political realities. The European Union, for example, has already adopted its own payment compliance requirements with the General Data Protection Regulation (GDPR) and, more recently, the Payment Services Directive 2 (PSD2) and the Anti-Money Laundering Directive (AMLD5). Other regions may follow suit, building their own payment compliance regimes that are tailored to their specific needs and interests.

It is also possible that one or more significant global payment compliance standards or frameworks will develop and be embraced by most countries and regions. This could occur if stakeholders agree that a unified strategy is required to assure interoperability and avoid fragmentation.

Given the volatile macro environment today, how do you think compliance priorities will change in 2023 and beyond?

The payment business is highly regulated, and compliance standards are continuously changing to keep up with new technology, changing customer behavior, and altering regulatory objectives. Some of the probable developments that could affect payment industry compliance in 2023 and beyond include -

Stronger regulations around digital payments: As digital payments become more prevalent, regulators may establish new laws to ensure that payment providers meet high security, fraud prevention, and consumer protection standards. To comply with these requirements, payment companies may need to invest in new technologies and processes.

Increased focus on anti-money laundering (AML) and counter-terrorist financing (CTF): Money laundering and terrorist funding are hazards to national security and financial stability in the payment industry. Regulators may increase their efforts to prevent such actions, which may include stronger KYC (know your customer) and due diligence requirements for payment providers.

Future developments in payment industry compliance may include stronger regulations for digital payments, heightened focus on anti-money laundering and counter-terrorist financing, increased emphasis on data protection, and expanded cross-border payment regulations.

Greater emphasis on data protection: Payment service providers handle sensitive personal and financial information, making them appealing targets for fraudsters. Payment providers may be required by regulators to employ stronger data security measures such as encryption, access controls, and regular vulnerability assessments.

Expansion of cross-border payment regulations: While cross-border payments represent a growing component of the payment industry, they are subject to complex regulations and compliance requirements. New restrictions may be enacted by regulators to ensure that cross-border payments are secure, transparent, and in compliance with local laws and regulations.

SISA Perspective

The role of AI in improving compliance and audit processes in the payments space

In the dynamic payments ecosystem, compliance and audit remain paramount for safeguarding financial transactions' security and integrity. The integration of AI technology revolutionizes these processes, enabling rapid and accurate analysis of large data volumes. AI empowers businesses to identify compliance issues, detect suspicious activities, and enhance overall compliance and audit processes in several transformative ways.

There are several other ways AI can be leveraged to improve compliance and audit processes, as indicated below.

Figure: AI Revolutionizing Compliance and Audit in Payments

Fraud Detection

AI can evaluate massive amounts of transaction data in real time, allowing financial organizations to spot patterns, abnormalities, and possibly fraudulent actions. Machine learning algorithms can learn from historical information, enhancing their capacity to detect fraudulent transactions accurately over time. By leveraging AI-powered fraud detection systems, financial institutions can swiftly detect and respond to fraudulent activities, mitigating financial losses and protecting their customers.

Risk Assessment

By utilizing machine learning algorithms, financial institutions can assess the risk associated with different transactions and customers. AI systems can analyze a wide range of data points, including transaction history, customer behavior, geographical location, and other relevant factors, to determine the level of risk involved. This proactive approach enables organizations to identify high-risk transactions or customers and take appropriate actions, such as applying additional security measures or conducting further investigation.

Regulatory Compliance

Regulatory compliance is another critical aspect of security in the payments industry, with stringent requirements imposed by authorities, including anti-money laundering (AML) and know-your-customer (KYC) regulations. AI can assist financial institutions in monitoring and ensuring compliance with these regulations. Machine learning algorithms can analyze large volumes of data, including customer information, transaction details, and external data sources, to identify potential violations and suspicious activities. AI systems can flag transactions that deviate from established patterns, enabling organizations to take corrective actions promptly and prevent non-compliance issues.

Audit Trail Analysis

Auditors can use AI to evaluate vast amounts of audit trail data by employing advanced pattern recognition and anomaly detection techniques. Unlike manual processes, AI-powered algorithms can process and analyze audit trail data from a variety of sources, such as logs, system records, and user activities, identifying irregularities that may indicate potential issues such as fraudulent activities, system breaches, or policy violations. Furthermore, AI-powered audit trail analysis can boost audit effectiveness by automating routine operations like data extraction and standard analysis, saving up auditors' time for complex investigations, critical judgements, and strategic decision-making.

Monitoring and Reporting

AI can automate transaction monitoring, ensuring compliance with regulatory requirements. AI systems can generate comprehensive reports that provide insights into compliance status, potential risks, and emerging trends by continuously evaluating transactional data. These reports help businesses remain on top of regulatory requirements, make informed decisions, and demonstrate compliance to auditors and regulatory bodies.

Predictive Analysis

AI systems can detect potential compliance concerns before they occur by leveraging historical data and machine learning algorithms. These forecasts can be based on the identification of patterns, risk indicators, or anomalies that suggest probable noncompliance or fraudulent activity. Armed with these insights, businesses can take proactive steps to address and mitigate identified risks, reducing the effect of any compliance violations and thereby protecting their reputation.

AI has enormous potential in the payments industry, particularly in the area of compliance and audit. By automating many of the manual processes involved in compliance and audit, AI can help companies stay ahead of the ever-changing threat landscape, reduce the risk of financial crime, and ensure that payment systems are secure and compliant. The integration of AI into compliance and auditing strategies is a crucial step for businesses striving to modernize their efforts in the face of an increasingly complex and ever-changing threat landscape.

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

Payment Data Security

- 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

- CCPA
- GDPR
- HIPAA
- ISO
- NIST
- SOC 1
- SOC 2
- Cloud Security

Security Testing

Application Security

- Application Penetration Testing
- CREST/CERT-in Approved Security Testing
- API Security Testing
- Secure Code Review

Network Security

- Vulnerability Assessment
- Penetration Testing
- Configuration Review
- Red Teaming Exercise
- Firewall Rule Review
- PCI ASV Scan
- Phishing Simulation

Hardware and IoT Security Testing

- Firmware Security Testing
- Hardware/Embedded Security Testing
- IoT Network Security Testing
- IoT/Embedded Application and Management Layer Security Testing

Cyber Resilience

Managed Detection and Response Solution – SISA ProACT

- Monitoring
- Attack Simulation
- Use-case Factory
- Advanced Threat Hunting

Digital Forensics and Incident Response

- Incident Response / Compromise Assessment Services
- Forensic Readiness Audit
- Forensic and Incident Response Retainer Service
- Payment Forensics Investigation
- Internal Forensics Investigation
- Ransomware Simulation

Data Security & Governance

Data Discovery and Classification - SISA Radar

- Card Data Discovery
- PII (Privacy) Discovery
- Data Classification
- Data Masking/Encryption

Data Security as a Service

Cyber Academy

Payment Data Security Implementation

- CPISI
- CPISI Advanced
- CPISI-D (Developers)

Security Incident Detection and Response Programs

- CIDR

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**