



PCI London 2027

January 20th, London, UK

Adapt or die: payment security programmes for the age of AI

The payments ecosystem left credit card data behind long ago. Can PCI DSS compliance deliver true payment security?

Bridging the gap between attestation and risk management

PCI DSS v4.0.1 has been fully in force since March 2025, and **the first full assessment cycle has taught hard lessons**: scope was broader than expected, the customised approach was harder to operationalise, evidence demands grew, and third-party contracts proved the weakest control.

The Council has begun work on v5.0 — with AI systems and modernised validation among its stated goals, but no publication date — and the PTS POI v5 device deadline has slipped to April 2027. The standard is moving from a point-in-time audit to continuous assurance faster than most compliance teams can staff it.

Meanwhile, the payment environment has moved beyond a neat cardholder-data perimeter. Modern payment journeys rely on JavaScript, hosted fields and iframes, mobile SDKs, APIs, cloud platforms, token vaults, fraud engines, digital wallets, orchestration layers and multiple third-party processors. Scope can be reduced, but dependency cannot. A merchant may outsource the checkout and remain exposed to compromised scripts, weak integrations or failures elsewhere in the payment chain.

Agentic commerce — AI agents authorised to shop and pay on a customer's behalf — is arriving and raises a question the standard has yet to answer: who is the cardholder when an agent pays? And the criminals have not gone away: browser-side skimming still harvests card data from checkout pages that passed their last scan, and the social-engineering playbooks that dismantled major retailers in 2025 bypassed every compliance control en route to payment systems.

That makes payment security a visibility problem as much as a compliance problem: what can touch a payment, who can change it, which systems and suppliers can influence authorisation, and how quickly will a control failure be detected?

The schemes and regulators add urgency. Enforcement of v4.0.1 is now real; reimbursement rules for authorised push-payment fraud have moved cost onto payment firms; and operational-resilience and third-party regimes on both sides of the Channel are pulling processors, cloud providers and managed service providers into the same conversation. But compliance is not security, and an attestation is not a control.

Compliance leaders face an external challenge (a payments ecosystem changing shape beneath the standard) **and an internal problem**: how to fund continuous assurance for one small dataset in organisations that believe the box is ticked — and how to get the same outcome for the small and medium-sized merchants making up most of the ecosystem.

Their case for action is not that PCI DSS has failed, but that **the gap between attestation and exposure is widening**: more suppliers, more channels, more automation, less human line of sight. Waiting for the next breach to reopen the budget conversation may be the mistake.

Where do PCI leaders see genuine assurance, where is a clean attestation masking hidden scope, and what practical steps should organisations take before v5.0 makes them mandatory? Is PCI DSS keeping up with payments — and are compliance teams keeping up with PCI DSS?

PCI DSS is at a crossroads: payment security is moving from proving compliance once a year to demonstrating control every day, across systems, suppliers and agents the compliance team does not own. PCI London will look at how compliance must deliver real security.

From point-in-time to continuous assurance

v4.0.1 moved the standard from annual audits towards ongoing monitoring and evidence, and the first full cycle showed how much that costs. Compliance teams need tools and processes that prove security every day, not once a year, with implications from basic workflow to risk management. **Can you help?**

Third-party and service-provider risk

Processors, gateways, cloud providers and MSPs all carry PCI obligations, and weak contracts, unclear SLAs and limited audit rights create blind spots that v4.0.1 exposes. Operational-resilience and critical-third-party regimes are now asking the same questions. **Any success stories in continuous supplier assurance?**

Automation, AI and evidence at scale

Manual evidence gathering and fragmented monitoring do not scale. AI and automation can streamline assessments, monitor scope, detect anomalies and embed PCI DSS into daily operations — but the Council is clear that human accountability and traceability are non-negotiable. **So, what is best practice here?**

Reducing the cost of compliance

Most organisations have limited resources, and the ecosystem is mostly small and medium-sized merchants completing self-assessment questionnaires. They need automation, solutions that apply more widely, and pro-business answers. **How do you derive PCI DSS compliance from the security processes you already run?**

Agentic commerce: who is the cardholder when an agent pays?

Schemes are building rails for AI agents that shop and pay on a customer's behalf, with delegated credentials and tokens. Authentication, consent, liability and scope were all designed for humans. **What does compliance look like when the customer is software, and can you help merchants prepare?**

Dealing with regulations

Teams now must build a single coherent security program that simultaneously satisfies divergent regulatory demands; they must interpret vague legal standards into technical architectures, and they risk non-compliance if auditors, regulators, or courts interpret differently later; they face unrealistic expectations around incident reporting; and they face personal liability. **Can RegTech help?**

Key Themes

Aligning PCI with the wider security and resilience stack

Compliance chiefs are under pressure to show that PCI DSS maps into NIST, ISO, GDPR, operational resilience and regulatory expectations. Integrating PCI into the enterprise risk stack turns compliance from burden into advantage. **But is PCI DSS really the right standard for this?**

Preparing for PCI DSS v5.0

The Council has signalled work on v5.0, with AI systems and modernised validation documents among its goals and no date yet. The cryptographic inventory now required under v4.0.1 is also the starting point for post-quantum migration. **What should compliance teams do now that will still be right when v5.0 lands?**

Scope: finding the CDE you did not know you had

Backup servers, monitoring tools, contact-centre recordings and data lakes have all turned out to be in scope. Discovery tooling, tokenisation and P2PE shrink the environment; late discovery is the most expensive remediation of all. **How do you find, reduce and keep control of scope continuously?**

Post-quantum readiness – really?

How do organisations improve cryptographic visibility and prepare for migration without creating operational risk? The new KMO standard provides a concrete development to examine: it addresses lifecycle key management and cloud-based or remote HSM use. **But is post-quantum readiness a practical planning discussion or pie-in-the-sky?**

Securing the contact centre and the human channel

The 2025 retail attacks went through help desks and identity, not zero-days. Voice deepfakes,, pause-and-resume and phishing-resistant authentication for operators are now part of the payment perimeter. **How do you keep agents, and their credentials, out of scope and out of reach?**

Browser-side skimming

Securing e-Commerce isn't just about payment card data or even pure payments. Script inventories, integrity checks and tamper detection are now mandatory, yet checkout pages that passed their last scan are still harvested through third-party and supply-chain scripts. Content security policies help; monitoring is what catches the change. **What actually works at scale, and at what cost?**

Why AKJ Associates?



A History of Delivery

For more than 25 years, AKJ Associates has been running the world's most sophisticated closed-door meeting places for senior cyber-security professionals from government, law enforcement, intelligence and business.

For example, our annual London-based e-Crime & Cyber Security Congress is still **the largest invitation-only, Chatham House rules**, gathering of the most senior information risk and security professionals from business and government in the world.

The UK Home Office sponsored the public sector delegation from 40 countries in 2002, and we are delighted to say they still do today.

Global Engagement

We have run hundreds of events in the **UK, across Europe, the Middle East and Asia**, attracting **tens of thousands of delegates** in cybersecurity, data security and privacy.

These delegates range from C-suite CIOs, CTOs, CROs and CISOs, to heads of enterprise architecture, desktop and network. They encompass all the senior professionals whose input drives security and privacy solution purchase decisions.

And as well as cross-sector events for both private and public sector, we also design and deliver sector-specific conferences for high-value, high-sophistication sectors including the legal sector, financial services, manufacturing, retail, healthcare, CNI.

Unrivalled Relationships

Events like this have enabled us to build relationships of trust with **the most influential decision-makers** at the full spectrum of public and private sector organisations in the UK, Europe, Asia and the Middle East.

By providing this audience with valuable insights and business intelligence over the past 25 years, we have built up **the world's most significant community of professionals in cybersecurity**.

We use this to develop new events; to conduct research to understand what cybersecurity professionals are doing, thinking and buying; and to market our conferences and other services.

Smart Lead Generation

We have also developed and trained one of the **most effective marketing and telemarketing operations** in the cybersecurity space.

Our in-depth knowledge of the marketplace allows us to design marketing outreach that **consistently delivers the best audiences** for the providers of critical cybersecurity infrastructure and solutions.

We connect vendors directly with B2B decision-makers. By combining unrivalled reach, deep knowledge of specialist markets and sophisticated marketing we **engage buyers to deliver real results**.

Delivering your message direct to decision-makers

Plenary Speakers

The e-Crime & Cyber Security Congress Series events offer sponsors the opportunity to deliver content in a number of different ways.

Plenary speakers **deliver their presentations on the day of the event from a fully featured AV stage to a face-to-face audience.**

Their presentations can contain slides, video and audio and speakers can deliver their speeches from the podium or from any point on the stage.

Plenary presentations are 20 minutes long and take place in the main event auditorium guaranteeing access to the largest possible audience of cybersecurity professionals on the day.

Presentations are generally designed to be informative, topical and actionable, with the use of case studies and up-to-the-minute references to current developments.

Double-handed talks with clients are also welcomed.



Education Seminars

At pre-defined points in the day, attendees will be notified that the main plenary sessions are making way for a series of in-depth technical break-outs.

These sessions of up to 30 attendees are held in break-out rooms and delivered live to attendees.

They are an opportunity for vendors to deep-dive into a topical problem, technology or solution in front of a group of cybersecurity professionals who have self-

selected as being interested in the topic being discussed.

They are also the ideal venue for solution providers to go into technical detail about their own products and services.

These Seminars run simultaneously, and attendees choose which session to attend.

At the end of the Seminar, attendees are notified that Networking time is now available before the next Plenary session.



Your team and your resources available in real-time

Exhibition Booths

Sponsor packages that contain an Exhibition Booth give sponsors the opportunity to be present in the main networking area of the event.

At these booths, sponsor representatives can interact with delegates face-to-face, deliver messaging and technical information via video presentations, demo products using their own BYOD technology and to distribute printed marketing and product information.

Sponsors may wish to consider different ways to drive footfall to their booths.

For example, sponsors who have presented in Plenary or in an Education Seminar can close their presentations by directing the audience to their booths.

And there are additional gamification elements available, including sponsor-supplied prizes, that can effectively drive traffic to booths.



Delivering the most senior cybersecurity solution buyers



Our USP? We put buyers and sellers together

We understand that every vendor needs to sell more. That is the bottom line. This is even more necessary in the present situation.

You will have access to the most senior buying audience in the cyber-security market.

AKJ Associates has been building relationships with senior information risk and security professionals for 25 years and our cybersecurity community is the largest of its kind globally.

We know the senior executives who drive strategy from the top, we know the enterprise architects who often control the largest budgets, and we know the IT Security Leads and Engineers who so often dictate the purchase process.

All of these job titles attend e-Crime & Cybersecurity Congress events.

Getting access to the right people at the right time always increases lead generation and always increases profitable sales activity.



PCI DSS & Compliance

We attract Heads of PCI, compliance leaders and assessors responsible for standards, audit readiness and continuous assurance



Payments Security

We bring together CISOs, payment-security leads and card-data protection experts securing the payment environment end to end



Fraud, Risk & Resilience

We convene fraud, operational-risk and resilience leaders addressing APP fraud, third-party exposure and control failures



Payments & Digital Commerce

We reach senior payments, e-commerce and digital-channel owners overseeing checkout, gateways, integrations and customer journeys

AKJ Associates

We deliver the most focused selling opportunity



Specific, actionable and relevant information for
time-constrained industry professionals



The perfect platform for solution providers to deliver tailored
advice to the right audience

Focus

Target growth

Each event represents a targeted opportunity to address the needs of a specific community whose need for your solutions and services is growing.

Leads

Boost sales

Sponsors can tailor messages to the needs of an audience that shares similar concerns and challenges, looking for solutions now.

Choice

Meet commercial aims

We work with sponsors to ensure they meet their commercial aims. We offer a number of sponsorship options, each providing specific benefits.

Value

Showcase solutions

Our events provide sponsors with a unique platform to showcase solutions, as well as provide advice on how best to solve delegates' key challenges.

AKJ Associates

Delegate Acquisition

- The e-Crime & Cybersecurity Congress has the **largest community of genuine cybersecurity stakeholders** to invite to our events.
- Our reputation for hosting **exceptional events with informative content, excellent networking opportunities and the best vendor partners** means delegates know they are attending a quality event and are willing to give up the time to attend.
- Our delegates are **invited by an in-house delegate liaison team** who call senior security and privacy professionals at public and private sector companies with a personal invitation to attend
- We **follow up all registrations** with further calls, emails on logistics requirements and reminders to **ensure the best possible attendance.**

Lead Sourcing

- The e-Crime & Cybersecurity Congress prides itself on **putting the key cybersecurity buyers and sellers together**
- To offer you the best prospects to network with, **we don't invite academics, job seekers, consultants, non-sponsoring vendors or marketing service providers** to this closed-door event. This **attention to quality over quantity** has been the hallmark of AKJ's events for 25 years.
- Each of our vendor partners will receive a delegate list at the end of the event.
- Through our targeted networking breaks built into our agendas you will have **unrivalled opportunities to network** with high-quality prospects with face-to-face networking at the event.

Get Your Message Across

- **Content is king**, which is why the e-Crime & Cybersecurity Congress prides itself on delivering informative and useful content, to attract senior audiences of decision-makers.
- Deliver an exclusive 20-min keynote presentation in the plenary theatre, or host a 30-min targeted workshop session: good content drives leads to your booth, and showcases your company's expertise
- AKJ's in-house content / research team will complement the agenda with best practice from leading experts and senior security professionals from the end-user community
- If you are not presenting, the exhibitor booth offers the opportunity to share white papers and other resources for delegates to takeaway

Exclusivity Delivered

- AKJ Associates has never done trade shows. We see most value in working with a **select number of the top vendor partners** and offering those companies the best access to leads.
- Our events keep the same ethos as when we first started 25 years ago, limiting vendor numbers. We will not be a hangar with hundreds of vendors competing for attention. We will keep our **events exclusive to give the best networking opportunities.**
- All booths offer the same opportunities with the same capacity and functionality regardless of the vendor company.
- This is an opportunity to **continue building pipeline and driving leads** in partnership with our outstanding 25-year reputation and the e-Crime & Cybersecurity Congress brand.

What our sponsors say about us



"Firstly, a big thank you for yesterday — it was a fantastic event, and we really felt it was a great success. The quality of the attendees was excellent; people were genuinely engaged and very open to conversation. We had strong interest at the stand throughout the day, with many visitors eager to learn more about our solutions."

Sales Manager UK & I



"Thank you for your email. I attended the event yesterday and have to say it was very well organised."

We were very happy with the turnout for our afternoon session as well - all in all, it was a very successful event!

Senior Marketing Executive



"AKJ are a pleasure to work with."

A lot of work goes into making physical events a success, and with AKJ the team are there to support at each step.

They ensure the events are a great success for both suppliers and end users alike."

Senior Digital Marketing Manager



"AKJ has been a valuable partner for us for a few years now, enabling us to build relationships and engage with the CISO community in a number of key territories across Europe. The events they hold are a great vehicle for discussing the latest challenges and our work with them has delivered way beyond expectations."

Senior Marketing Manager

95% percent of our exhibitors and sponsors work with us on multiple events each year.

This is because they generate real business at our events every year. Our sponsor renewal rate is unrivalled in the market.

AKJ Associates