



27th PCI London: meeting the challenge of 4.0.1

January 21st, 2026, London, UK

PCI DSS v4.0.1, the challenge of continuous assurance and the rise of AI

Meeting the demands of 4.0.1 is hard and non-stop technology innovation isn't helping.
What are the best organisations doing?

Tougher than you thought? How organisations have responded to PCI DSS v4.0.1

Early adopters of PCI DSS v4.0.1 have reported that the journey has been harder and more resource-intensive than expected. Many organisations underestimated how broad their cardholder data environments (CDEs) are, and how many connected systems — from backup servers to monitoring tools — fall within scope. Discovering these dependencies late in the process has led to costly remediation.

Technical complexity is high. Stronger authentication requirements, stricter cryptography, more comprehensive logging, and expanded monitoring have required major upgrades.

The “Customized Approach” has caused some confusion. PCI DSS v4.0.1 allows organisations to propose alternative controls that meet the intent of requirements, rather than follow the exact “Directed Approach.” While flexible, this option has been difficult to operationalise.

Future-dated requirements are a double-edged sword. Those who delayed action are now facing resource bottlenecks.

Third-party and vendor risk is a critical weak spot. Payment data often passes through vendors, processors, or cloud providers. Many contracts do not yet bind these third parties to PCI DSS v4.0.1-level obligations. Service providers with older systems often cannot support the required controls without significant investment.

Documentation and evidence demands have grown. Under v4.0.1, compliance chiefs must maintain logs, configuration records, change histories, and detailed evidence of testing.

Organisations that treated compliance as an annual “checkbox” exercise have had to rethink their entire documentation approach.

E-commerce merchants have faced new requirements to control third-party scripts. Without monitoring for script tampering, merchants risk data skimming attacks. Those who implemented script inventories, integrity checks, and content security policies have both met the new standard and improved customer security.

Across sectors, compliance chiefs have reported similar pain points: vendor contract weaknesses, underestimation of scope, confusion over customized controls, and the heavy lift of continuous monitoring.

In parallel with PCI DSS v4.0.1, the PCI SSC has begun addressing the impact of artificial intelligence on compliance and payment security. The core message is simple: AI can help, but it cannot replace human accountability. In assessments and in payment environments, the Council makes clear that human accountability, traceability, and resilience planning are non-negotiable.

For solution providers, the opportunity is clear. Compliance chiefs are actively searching for tools and partners who can:

- **Automate compliance evidence collection and reporting.**
- **Deliver robust access control, encryption, and monitoring aligned with v4.0.**
- **Provide script monitoring and integrity solutions for e-commerce.**
- **Integrate AI safely into assessments and payment ecosystems.**
- **Help manage vendor and third-party risks.**

PCI London will continue our look at PCI DSS 4.01 and the progress compliance teams are making. Join our real-life case studies and in-depth technical sessions from the PCI compliance leaders at a broad cross-section of organisations and sectors.

Key Themes

From point-in-time to continuous compliance

PCI DSS v4.0.1 moves away from annual audits towards ongoing monitoring and evidence. Compliance chiefs must adapt to continuous assurance, with tools and processes that prove security every day, not once a year. This has implications across the security and compliance estate, from basic workflows to complex risk management. **Can you help?**

Aligning PCI with broader security frameworks

Compliance chiefs are under pressure to show that PCI DSS maps into broader obligations — NIST, ISO, operational resilience, 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?**

Tackling PCI DSS v4.0's new requirements

From targeted risk analyses to stronger authentication, encryption updates, and enhanced testing, v4.0.1 introduces significant new technical and procedural demands. Organisations must understand not just what has changed, but how to implement it effectively. **What tools should they look at?**

New challenges in managing third-party risks

Processors, merchants, and cloud providers all bring PCI DSS obligations. Weak contracts, unclear SLAs, and limited audit rights create blind spots. Third-party management is one of the toughest and most critical challenges under v4.0. But then it's probably the hardest challenge in cybersecurity and operational risk too. **Any success stories?**

Technology challenges in hybrid environments

Payment systems now span legacy POS, APIs, mobile, and cloud providers. Extending PCI DSS controls across such diverse and interconnected environments is complex — especially when vendors or legacy systems can't easily comply. **How can organisations comply in this situation?**

Automation, AI & continuous assurance

Manual evidence gathering and fragmented monitoring won't scale. AI and automation offer opportunities to streamline assessments, monitor scope, detect anomalies, and embed PCI DSS into day-to-day security operations — but only if used responsibly. **So, what is best practice here?**

Key Themes

Reducing the cost of PCI DSS compliance

Most companies have limited resources to devote to one small dataset (card data). They need solutions that can be applied more widely, they need automation, and they need pro-business solutions. Surely this is the wrong way round? **So, how do you derive PCI DSS compliance from your existing security processes?**

Securing Cloud and other critical third-party dependencies

PCI DSS 4.0.1 allows firms to choose their path to delivering the security and privacy objectives set by the standard. It then specifies how organisations can demonstrate that their chosen solutions do indeed deliver those outcomes. **How can you help?**

Vulnerability Management and remediation

Firms need to know where the greatest risks to their data lie and how best to mitigate them. To do this they need network and process visibility, third-party visibility and good technology to cover new payments channels and platforms. **Can your solutions help them?**

New technologies – a challenge to compliance?

The world of payments is in flux. From Klarna to Stripe, from Wise to wallets, the tools we use to make payments and the channels through which card data flows are changing. **How much do these innovations change the nature of PCI DSS compliance and can you help?**

Aligning PCI DSS, GDPR and broader GRC efforts

Companies have spent significantly on PCI DSS, then poured more into other compliance initiatives. What commonalities tie their different compliance goals together and which technologies can save them money while keeping them secure? **Can you provide help or advice or solutions in this area?**

Technology investment decisions are getting harder

All compliance regimes evolve as the wider marketplace does. Keeping up is a constant struggle. But with PCI DSS 4.0.1 promising a new risk-based approach, will yet another round of investment be needed? **Can your solutions ease the transition?**

Why AKJ Associates?



A History of Delivery

For more than 20 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 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 and gambling and gaming.



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 20 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 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.

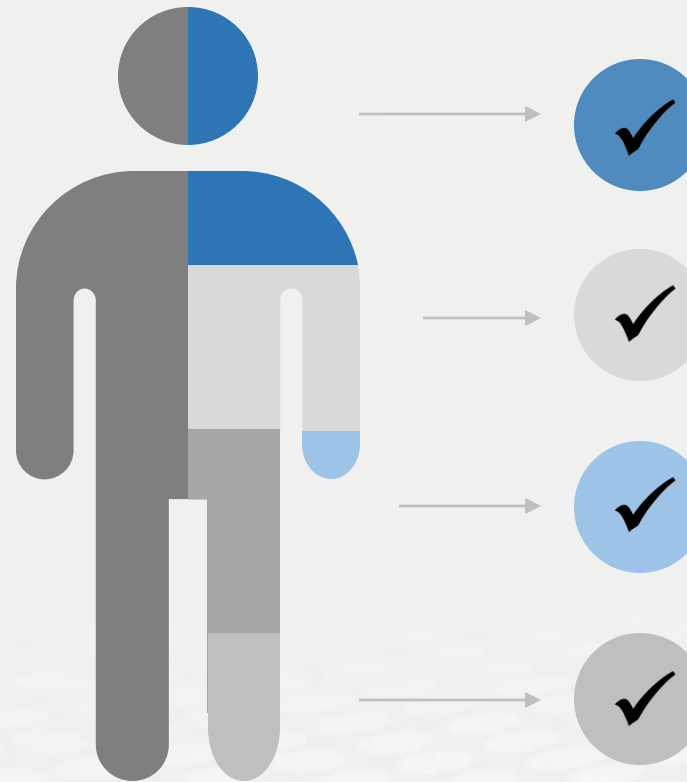
You will have access to the most senior buying audience in the cyber-security market.

AKJ Associates has been building relationships with senior information risk and security professionals for 20 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 PCI London.

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



Cyber-security

We have a 20-year track record of producing the events cyber-security professionals take seriously

Risk Management

We attract senior risk officers with responsibility for information risk assessment and mitigation

Fraud, Audit, Compliance

We provide the go-to events for fraud prevention and compliance owners at the world's key corporates

Data Protection & privacy

We are a key venue for decision-makers with budget and purchasing authority

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.

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 20 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 virtual 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 20 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 20-year reputation and the e-Crime & Cybersecurity Congress brand.

What our sponsors say about us



It was indeed a great show. Despite the situation overall [COVID 19] the number of people that turned up, shows the trust people have of the e-Crime brand. Wish you all the best for the upcoming events and we shall surely be a part of them.



This is always a great event for 'taking the temperature' on security issues, to get a feel for people's impressions on current security challenges and to find out what organizations of all kinds are doing.

The logo for VMware Carbon Black, featuring the text 'vmware Carbon Black' in white on a blue rectangular background.

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 opportunities in the security sector, and our work with them has delivered way beyond expectations.

✓ **Ninety five percent of our exhibitors and sponsors work with us on multiple occasions each year**

✓ **Our sponsor renewal rate is unrivalled in the marketplace**

✓ **This is because our sponsors generate real business at our events every year**

AKJ Associates