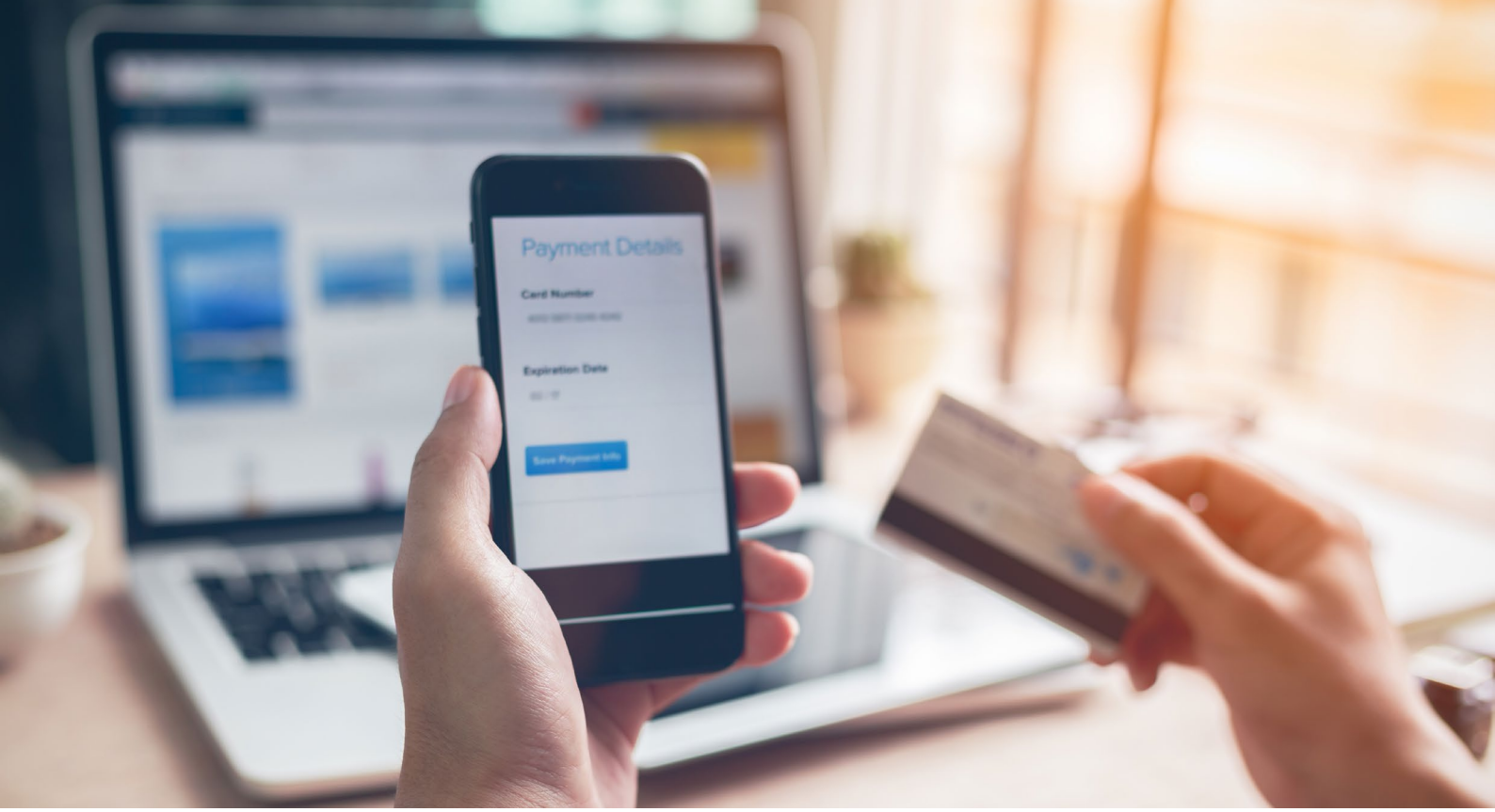
Beyond PCI DSS compliance: Assessing and shrinking enterprise risk

An expert's guide for security leaders in the APAC region

verizon business



With Asia-Pacific (APAC) on track to become a $1 trillion digital economy by 2030[1], mainly driven by the surge in cashless and instant payments, Chief Executive Officers, Chief Financial Officers, and Chief Information Security Officers remain anxious about the implications of mandatory data breach reporting and the forthcoming implementation of the global and universal Payment Card Industry Data Security Standard (PCI DSS) v4.0.

In a climate of uncertainty, Verizon advisory services can help businesses master these compliance challenges.

- As a security leader, your task is challenging: You're in a region hit by over a third of all cyber attacks worldwide[2], making it the top target.

The Verizon 2024 Data Breach Investigations Report shows that financial services are the second most attacked sector, with 9 out of 10 attacks targeting Japan[3].

With PCI DSS v4.0, we're tackling not just technical hurdles - 64 new requirements[4] - but also the weight of shareholders' expectations in larger companies, demanding greater transparency and security regarding data breaches and zero-trust progress.

Australian CEOs could see their companies face penalties of up to 30% of their annual adjusted turnover if their team fails to safeguard data effectively - from the trading or factory floor to the C-suite.

In one recent APAC incident, a Singaporean online retail platform[5] experienced a significant data breach exposing the credit card details of 2.76 million customers, leading to unauthorised transactions and financial losses.

The company then suffered reputational damage and potential regulatory fines, emphasising the high stakes of data security in the digital payment ecosystem.

This breach includes four specific gaps in their approach when matched to PCI DSS v4.0 standards (which total 12 core data security requirements)

1. Requirement 3 (Protect Account Data): Failure to adequately encrypt or mask stored payment data.
2. Requirement 7 (Restrict Access to Cardholder Data): Insufficient access control measures allow unauthorised access to sensitive information.
3. Requirement 9 (Physical Access to Cardholder Data): Lapses in securing physical systems and environments where cardholder data is processed or stored, leading to potential unauthorised physical access.
4. Requirement 11 (Security Testing): Inadequate regular testing of security systems and processes exposes enterprises to breaches and further vulnerabilities.

While these show specific gaps in compliance, the more significant problem is building a unified

1 https://www.cnbc.com/2023/11/29/southeast-asia-may-be-on-the-cusp-of-a-cashless-payments-revolution.html
2 https://www.ptsecurity.com/ww-en/analytics/asia-cybersecurity-threatscape-2022-2023/
3 https://www.verizon.com/business/resources/reports/verizon-vision-for-banks-enterprise-intelligence-anz.pdf
4 https://listings.pcisecuritystandards.org/documents/PCI-DSS-v3-2-1-to-v4-0-Summary-of-Changes-r1.pdf
5 https://www.pdpc.gov.sg/all-commissions-decisions/2023/03/breach-of-the-protection-obligation-by-eatigo-international

and efficient approach to compliance and risk management that dynamically evolves over time.

Many businesses are operating with fewer resources, often using trial and error to meet the requirements for a standard designed to protect cardholder data across merchants, third parties and customers.

Add in inadequate stakeholder buy-in, unclear program objectives, and underestimation of the program's complexity, and it will likely become more difficult to keep up and stay systematically ahead of security standards.

Ongoing protection of payment data requires maintaining existing security controls while implementing changes for PCI DSS v4.0.

Over half of all big companies worldwide, earning over US$10 billion annually, faced fraud in the last two years. Even more shocking, about one in five of these companies said their biggest fraud issue cost them over $50 million6.

Unless you make disclosure and compliance your north stars today, you risk crippling your company during a period of massive digital uncertainty.

However, embracing a focused action plan for compliance allows enterprises to achieve breakthrough performance enhancements in security program design.

Turning gaps into opportunities

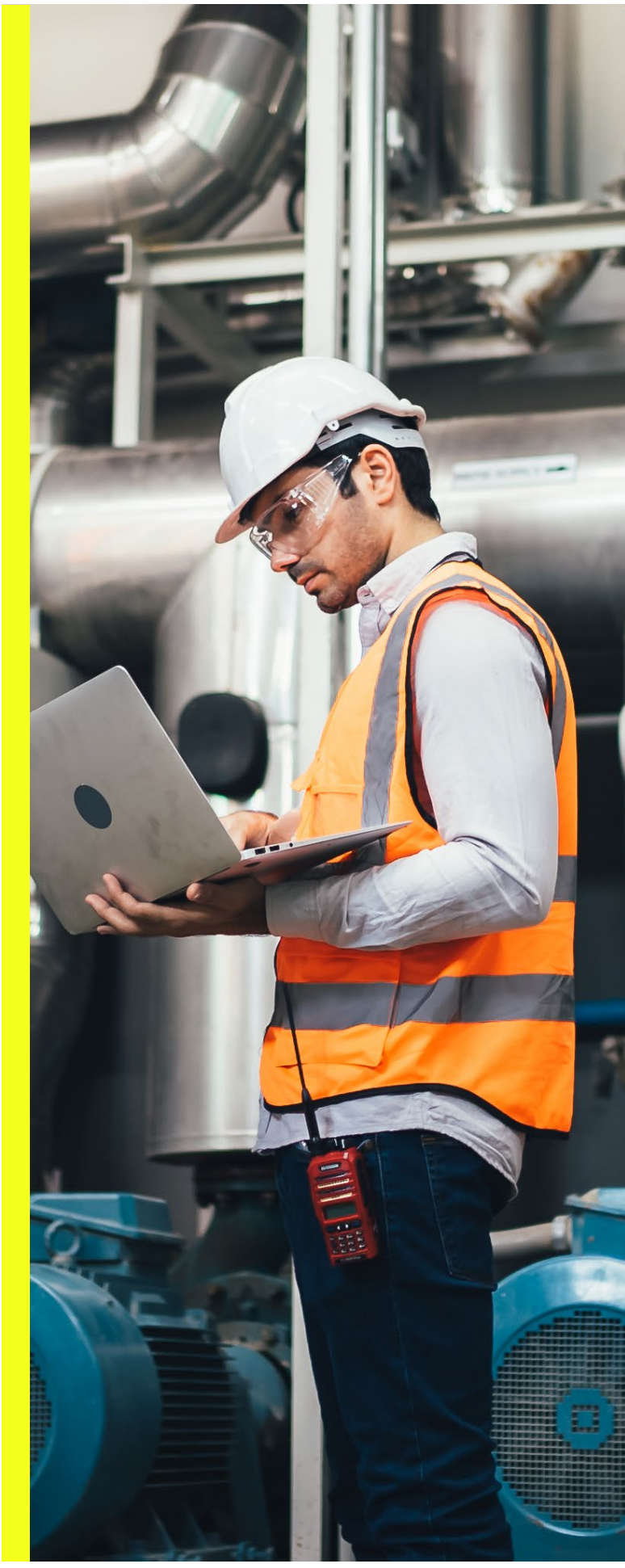
Using the United States (U.S.) as a lens, we highlight compliance gaps and opportunities for the APAC region.

Around 17% of cross-border transactions[7] within APAC originate from the U.S. highlighting the global nature of digital commerce and the importance of adhering to international security standards like PCI DSS v4.0 to ensure safe transactions across borders.

Even though most organisations in the U.S. had over a year to prepare for the 4.0 rollout, many boards are still anxious, with new cyber disclosure rules from the U.S. Securities and Exchange Commission requiring security leaders to report cyber incidents to the SEC within four days of determining that an incident is material.
Similar regulatory trends are rippling across APAC, highlighting the importance and urgency of building a transparent organisation that maintains sustainable control environments.

There is also the need for continual improvement to ensure adequate, ongoing protection of payment card data.

Building this roadmap to achieve compliance—and then maintaining it—is painful for many U.S. and APAC customers.



6 https://www.pymnts.com/news/b2b-payments/2023/incoming-payments-fraud-costs-companies-millions-every-year/#:~:text=Fraud%20is%20both%20costly%20and,costs%20more%20than%20%2450%20million.
7 https://www.enterprisetimes.co.uk/2021/10/28/digital-payments-in-europe-to-grow-by-70-says-new-ppro-research/

Whether you're at the stage of identifying PCI compliance gaps, already aware of these gaps and looking for solutions, need a thorough assessment of your current compliance status, or are eager to enhance your payment security with innovative tools and processes, it's time to take the next step forward.

Unscrambling compliance complexity

The critical piece in this cube of complexity is pre-assessments.

Verizon can help organisations balance the areas in which they excel, are on par, or fall behind.

This forewarning provides the opportunity to prepare for the PCI assessment thoroughly, using a practice exam approach.

Many CEOs are surprised to learn how poorly they perform in pre-assessments.

However, it becomes the first step in a transformative security metamorphosis and moving from a disjointed set of activities to creating a formalised program.

Principles driving compliance success

Amid the ever-changing and developing landscape of the last two decades, Verizon has shaped and continually improved its approach to PCI compliance and predictable performance, which is underpinned by four guiding principles:

- Eliminate waste
- Address low productivity
- Prevent high cost
- Avoid stakeholder dissatisfaction

Many businesses treat their PCI security checks as separate from their overall governance plans. They need to see how combining these streamlines activity and prevents the same tasks from being done twice in different programs.

Annual introspection

By coordinating all the different rules and regulations under one overarching governance strategy, we can strive to enhance compliance and effectively manage risks.

Companies should review their governance strategy every year, checking the goals, requirements, and limits they might have. This keeps things smooth and efficient.

A team of Qualified Security Assessors (QSAs) aims to help enterprise and public sector agencies overcome these hurdles:

- Maintaining organisational silos—hampering communication, performance and sustainability
- Focusing on technology, undervaluing processes and procedures
- Forgetting, underinvesting, rushing—inadequate organisational competency development
- Falling short on training and educational efforts

A unified approach can transform a project into a long-term security program that modernises payment systems and aims to provide resilient cyber protection from adversaries.

Building compliant cyber shields in APAC

Regular check-ups and a sharp, shared plan for safety can steer APAC companies clear of the cyber dangers spotlighted in the recent annual Data Breach Investigations Report (DBIR).

Social engineering

In the APAC region, 93% of security breaches stem from tactics like social engineering, hacking into systems, and exploiting vulnerabilities in essential web applications.

To counter these threats, PCI DSS v4.0 mandates stringent rules[8], such as fortifying network security, safeguarding payment information, strictly regulating data access, and conducting regular security assessments.

Financial motives

The DBIR highlights how financial motives drive 61% of these breaches[9], underscoring the imperative to secure payment data against credit card fraud. PCI DSS addresses this by mandating the encryption of payment data transmitted across the internet and ensuring the secure storage of such data.

The human angle

Breaches often involve the theft of sensitive information, including internal company data, trade secrets, and user credentials, highlighting the necessity for PCI DSS's requirement for data encryption, secure data storage, and the implementation of robust authentication mechanisms.

An overwhelming 92% of breaches within the 2024 DBIR data set are orchestrated by external actors, emphasising the need for robust external defences as outlined by PCI DSS.

However, internal actors are responsible for 9% of breaches in the same data set, reinforcing PCI DSS's emphasis on internal controls like access restrictions and activity monitoring to mitigate insider threats.

Adopting PCI DSS guidelines, such as implementing strong password policies and assigning unique IDs to each user, equips companies to shield vital payment information more effectively from unauthorised access, ensuring a more secure digital payment landscape.

8 https://www.pcisecuritystandards.org/
9 https://www.verizon.com/business/resources/T42/reports/2023-data-breach-investigations-report-dbir.pdf

Industry compliance

While our recent DBIR includes data from around the world, including North American sectors such as financial, insurance, retail, accommodation, and hospitality services, these findings offer valuable lessons for the APAC region.

Examining these industry data breach trends, APAC businesses can anticipate similar trends and vulnerabilities within their own markets.

It's crucial, however, to adapt these insights with a keen understanding of the unique regulatory, cultural, and economic landscapes across APAC countries.

This approach enables a holistic security vision that not only meets global compliance standards like PCI DSS but also addresses region-specific risks and opportunities for improvement.

Healthcare

Overview: The healthcare sector remains a prime target for cyberattacks. The DBIR highlights 525 incidents, with 436 confirmed data breaches, primarily due to system intrusion, basic web application attacks, and miscellaneous errors (Verizon DBIR, 202310). These threats underscore the urgent need for stronger cybersecurity in healthcare.

Key issue: Ransomware continues to plague this sector, compounded by internal errors like misdelivery that put patient data at risk.

PCI DSS 4.0[11] offers important countermeasures:

- Requirement 5.1: Up-to-date anti-virus – Crucial for blocking malware, often the initial stage of ransomware attacks.
- Requirement 9.4: Physical access controls – Limiting access to sensitive areas helps prevent both external intrusion and accidental data disclosure, a major internal threat.

While compliance doesn't guarantee immunity, it provides a robust defence framework for protecting healthcare information systems and sensitive patient data.

Manufacturing

Overview: Manufacturing is a high-risk sector, with 1,817 incidents and 262 confirmed breaches reported in the DBIR (Verizon DBIR, 2023). System intrusions, social engineering, and web application vulnerabilities pose significant threats.

Key Issue: External attackers, both financially motivated and seeking espionage opportunities, exploit hacking, malware, and social engineering techniques to target vulnerable manufacturing systems.

10 https://www.verizon.com/business/resources/T42/reports/2023-data-breach-investigations-report-dbir.pdf
11 https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

Stronger protections come from PCI DSS 4.0:

- Requirement 4.1: Secure data transmission – Mitigates attack risks by encrypting sensitive data during network transfers.

- Requirement 12.6: Security awareness program – Equips employees to identify and avoid social engineering tactics, a key attack vector.

Adherence isn't a one-time fix. Evolving with PCI DSS 4.0 builds resilience against the latest threats and safeguards manufacturing data.

Financial and insurance

Overview: The DBIR highlights the sector's vulnerability, with 1,832 incidents and 480 confirmed data breaches, primarily due to web application attacks (Verizon DBIR, 2023). This underscores the critical need for robust vulnerability management and patching.

Key Issue: Basic web application attacks continue to be a major threat, leaving financial and insurance data exposed.

Stronger protections from PCI DSS 4.0:

Requirement 6.4: Install vendor-supplied security patches – Mitigates attack risks by ensuring all system components and software are up-to-date with security patches from vendors.

Regular patching remains essential to address evolving threats and safeguard sensitive financial data.

Retail

Overview: Retailers remain vulnerable, with the DBIR showcasing 406 incidents and 193 confirmed data breaches, largely driven by system intrusions, social engineering, and web application attacks (Verizon DBIR, 2023). This highlights the importance of secure data storage and protection, especially for payment card information.

Key Issue: Cybercriminals specifically target payment card data, putting retail customers at risk.

Stronger protections from PCI DSS 4.0:

- Requirement 3.2: Store only necessary authentication data – Minimises the attack surface by mandating that only essential authentication data is stored.

Regularly review and minimise data storage practices to safeguard sensitive financial information.

Accommodation and food services

Overview: The sector reported 254 incidents with 68 confirmed data breaches (Verizon DBIR, 2023). Highly dependent on payment transactions, it faces a significant risk from RAM scraper malware used in 90% of breaches stemming from system intrusion, web application attacks, and social engineering.

Key Issue: The prevalence of RAM scrapers targeting payment card data highlights the need for advanced malware protection strategies.

Stronger protections from PCI DSS 4.0:

- Requirement 5.4: Protect systems from malicious software – Mandates the deployment and regular updates of anti-malware solutions for effective detection and prevention of RAM scraper attacks.

Regularly update and review anti-malware defences to ensure effectiveness against evolving threats.

Other sectors

The insights above just scratch the surface.

The DBIR continues with the sectors we've discussed; it covers much more, from educational services and mining to public administration and many other industries.

We encourage readers to explore these sections to enrich their knowledge and identify cross-industry patterns and solutions that might apply to their specific context.

Compliance across the cloud

Transitioning to cloud services for processing, storing, and transmitting cardholder data introduces a new layer of complexity in achieving PCI DSS compliance.

When sharing resources among multiple clients, it's essential to clearly define the responsibilities of both the cloud service provider (CSP) and the client in protecting cardholder data.

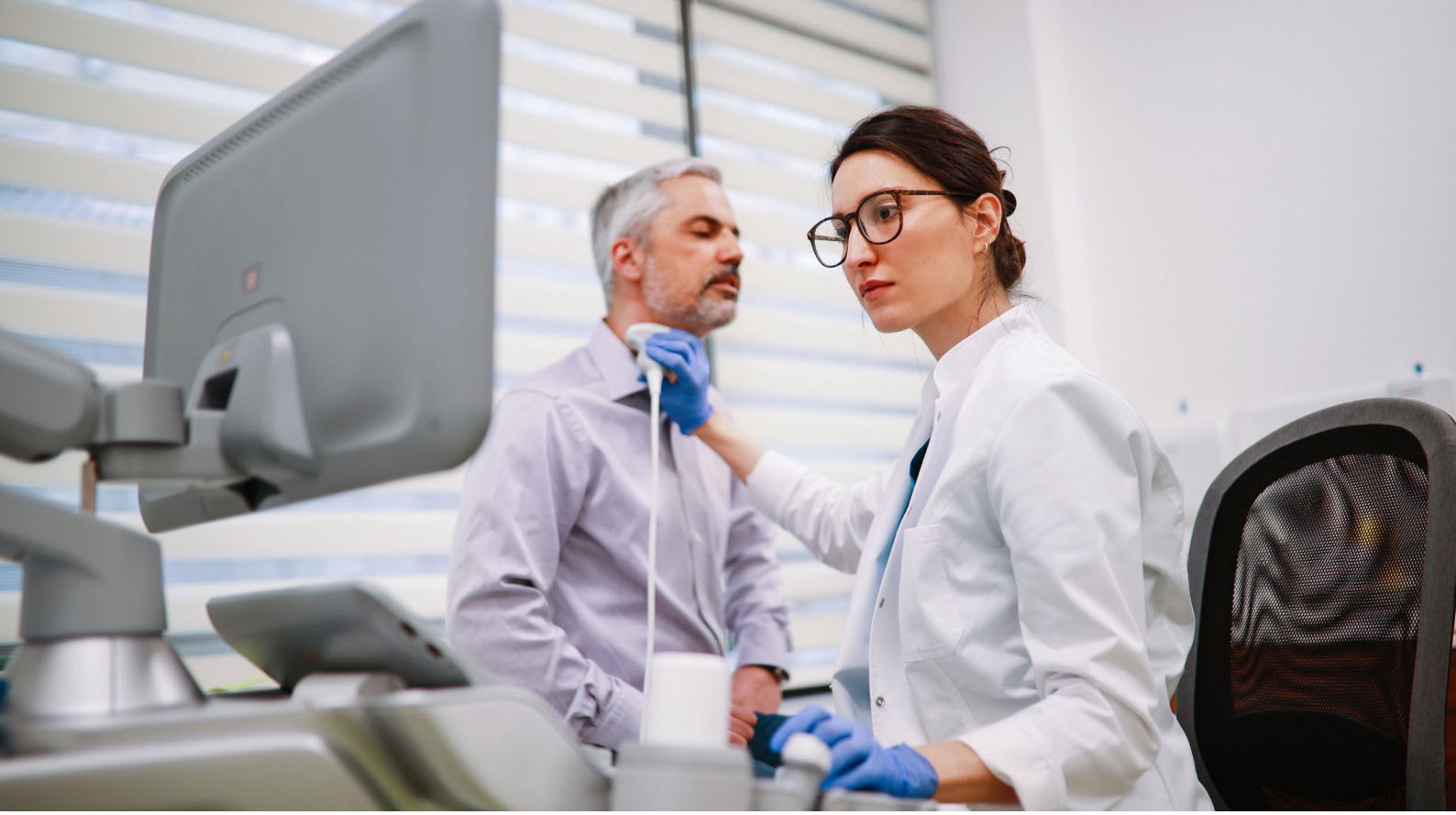
PCI DSS Requirement 12.8, for example, mandates that organisations maintain a list of service providers with access to cardholder data and a written agreement that acknowledges the providers' responsibility for securing that data.

Mapping the Cloud Controls Matrix to PCI DSS[12] ensures that cloud security measures align with payment data protection standards, enhancing the security posture of cloud-based payment systems and ensuring compliance with industry regulations.

The Cloud Controls Matrix (CCM) is a cybersecurity framework developed by the Cloud Security Alliance (CSA), of which Verizon is a member[13]. This membership aligns with our efforts to promote security within cloud services and contribute to developing best practices for cloud security.

The Verizon approach to cloud security involves a detailed mapping of CCM to PCI DSS, highlighting shared responsibilities and ensuring a comprehensive protection strategy.

12 https://cloudsecurityalliance.org/blog/2023/09/19/strengthening-cloud-security-mapping-the-cloud-controls-matrix-ccm-4-0-to-pci-dss-4-0
13 https://www.verizon.com/business/resources/solutionsbriefs/2020/security-risk-assessment.pdf



Verizon's cloud services integrate PCI DSS requirements, focusing on encryption, access control, and continuous monitoring to provide robust security for cardholder data in cloud platforms.

Benchmarks that matter

We understand that aligning with industry standards is a regulatory requirement and a strategic necessity.

With a global presence, including operations in Australia and nine other security operations centres, Verizon manages over 500,000 security and network devices, providing unparalleled insights into international and regional cybersecurity standards and the information and services necessary to stay ahead of potential threats.

Verizon Governance, Risk & Compliance (GRC) advisory services can help you measure and elevate your security program against these essential benchmarks:

- ISO27001/ISO27002: These standards form the foundation of a robust information security management system and are pivotal in enhancing PCI DSS compliance and safeguarding cardholder data against potential breaches.

- National Institute of Standards and Technology Frameworks: The comprehensive guidelines provided by NIST Technology Cybersecurity Framework and Special Publication 800-53 extend beyond compliance, focusing on risk management and security controls to fortify your defences against cyber threats, thereby supporting PCI DSS objectives.

Regional Compliance in APAC:

The APAC region presents unique challenges, with local regulations and standards introducing additional layers to PCI DSS compliance:

- The Australian Signals Directorate Essential 8: Implementing these strategies bolsters your security posture, indirectly facilitating PCI DSS compliance by reinforcing defences against prevalent cyber threats.
- Privacy Act 2018 Australia and New Zealand & Information Security Registered Assessors Program Certification: These frameworks signify a deep commitment to data protection, resonating with PCI DSS's core principles and enhancing the security of sensitive information.

Backed by certifications like Certified Information Systems Security Professional and Certified Information Security Management Consultant, Verizon embodies a deep-rooted understanding of these global and regional standards. This expertise, combined with extensive experience conducting over 19,000 security assessments, uniquely positions Verizon to help guide you through achieving and maintaining compliance.

Compliance by design

PCI DSS version 4.0 brings significant updates, including continuous assessments and better validation methods. It moves organisations from fixed rules to allowing flexible, goal-oriented strategies in its 10th release.

The scale and pace of changing complaint regulations also put overwhelming pressure on Chief Information Security Officers and internal IT departments.

When we conducted a payment security report a few years ago, we found that only 43% of companies met all compliance standards. It's understandably difficult not to take shortcuts or ignore blind spots that can leave you vulnerable to compliance failure, especially as you stretch your perimeter to the cloud and IoT environments.

Consequently, it no longer makes sense to keep every cybersecurity aspect in-house. A partnered approach enables CISOs to augment their core team with on-demand capabilities that are usually quite hard to find and maintain.

CEOs and boards now have peace of mind knowing that Verizon advisory service unearths overlooked areas while understanding how different security measures and their settings interact. This is a crucial goal of Verizon assessments for companies of all sizes, including many Fortune 500 and multinational organisations.

Ultimately, security leaders should never forget that data security and compliance success is achieved by design – not luck.