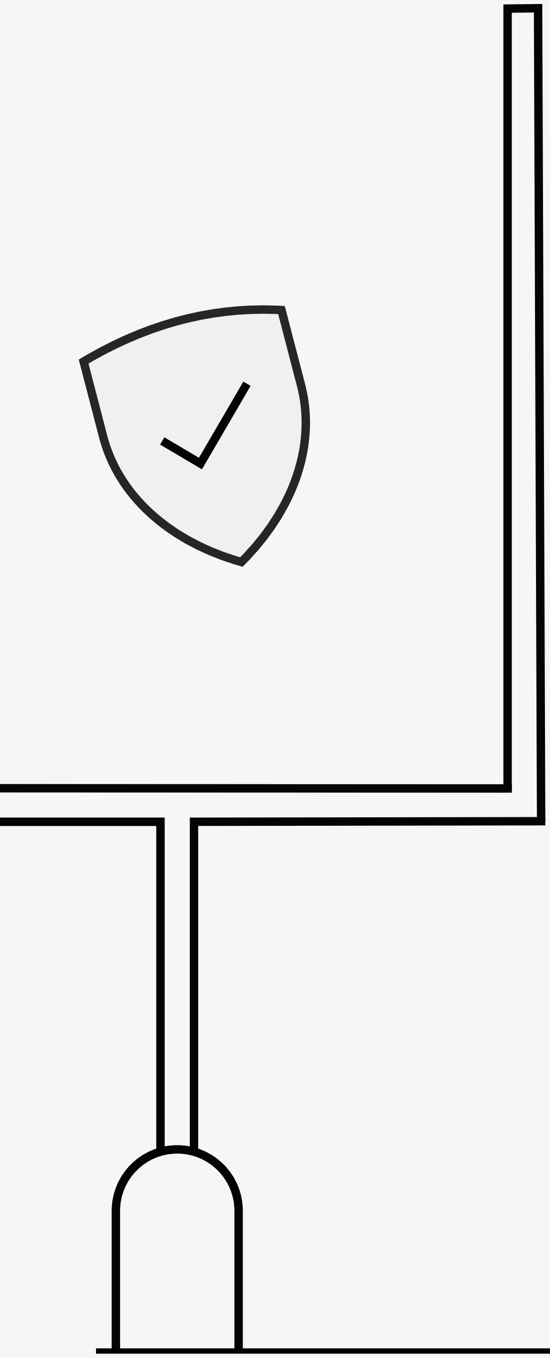
Appendices

Appendix A: Primer for crafting security and compliance goals

Goals come in many forms. The extent to which governance, risk management and compliance goals are accomplished is an indication of the capability maturity of an organization. Most security and compliance goals require multiple steps. Deconstructing a goal by breaking down specific actions is helpful in defining individual steps and achieving the finished result. It's important to apply a goal-setting method that helps you be highly specific when articulating goals and their requirements and constraints.



Below are various aspects of goals and objectives:

1 Types of goals and objectives:

- Short-, medium-, long-term goals
- Positive vs negative goals
- General vs specific goals
- Process- vs results-oriented objectives

2 Setting goal targets

- Minimum, average and maximum output

3 Eliminating and then refining your goals

4 The benefits of clearly defined goals

5 The connection between goals and productivity and the need for tradeoffs

Types of goals and objectives

Security and compliance goals can incorporate short-, medium- and long-term objectives designed to identify steps toward overall success. Goals typically present the big picture and, if they are not specific enough, may seem intangible because they are too broad or general. For instance, one of the goals for your business might simply be "24/7 protection of sensitive data in accordance with regulatory compliance requirements." With such a general statement, this goal may seem unattainable.

Determine your long-term security and compliance aims.

Start by distinguishing long- from short-term goals. Your long-term goals should have a timeline of three to five years. Long-term goals generally reflect your company mission and should be distinguished from short-term goals.

Break down each long-term goal into medium- and short-term objectives.

Similar to how you break down short-term goals, you will need to break down your long-term goals into actionable medium- and short-term objectives. A goal that remains unclear, not broken down into concrete objectives (partial goals), runs the risk of taking on a life of its own. Without concrete goals, there are no criteria that can be used to judge whether progress is, in fact, being made. For example, if your long-term goal is for every system component across your compliance environment to be demonstrably effective and sustainable, you will need to break this down into short-term objectives that ultimately will help you accomplish the long-term goal. Examples of actionable objectives for the above goal would be to prioritize the system components that can most impact the risk and security of CHD and ensure that the components are designed to operate in an effective and sustainable manner. Then, incrementally move on to improve other components to the desired level of effectiveness and sustainability.

Positive vs negative goals

In general, there are two different kinds of goals: positive and negative. With some security and compliance projects, you act to bring about conditions considered desirable. With others, you act to change, abolish or avoid conditions considered undesirable. To work toward a desirable state of affairs is a positive goal; to correct or prevent a deficient state of affairs is a negative goal. This is an important distinction. With a positive security and compliance goal, you want to achieve a definite condition. The organization pursues changes to bring about certain conditions that are considered desirable. With a negative goal, you want a condition to not exist. The intentions to avoid or change undesirable conditions (negative goals) – such as a payment card data breach – are often not well defined, but instead expressed in broad, rather vague terms.

General vs specific goals

You can also distinguish between general and specific goals. Typically, general (or generic) goals define broad primary outcomes and general security and compliance intentions and ambitions of the organization. They are comparatively easier to define and cover a larger scope – setting a wide, overarching target with a few or single criterion. However, they may be more difficult to measure. In contrast, specific goals are very precisely defined by many criteria. Specific goals lead to specific practices. Goals are more likely to be reached when they are clearly defined, with as much detail and specificity as possible.

Process- vs results-oriented objectives

Process objectives are like resolutions. The security team may resolve to allocate resources to spend a certain number of days per month assessing and documenting the status of controls, or they may decide to update a certain percentage of outdated systems each week.

Results-oriented objectives are usually dependent on processes or a series of actions, but are considered achieved based solely upon the outcome.

A security team may be successful in achieving an objective when all outdated systems are successfully upgraded. Another example would be when all required PCI DSS controls are fully documented across the control environment.

Unless standards are set very low, process objectives are more readily achieved than the results-oriented objectives, because processes are more controllable than outcomes. Organizations that have the skills and experience to achieve a certain result find it easier to design their activities to assure that they reach their objectives and goals.

PCI security management: Setting goal targets

When you establish goals for your security and compliance program, there are several different ways you can go about it.

Minimum output

The first way is to target the minimum output for your PCI security program. Typically, this means doing only what is necessary to avoid failing a compliance validation assessment. However, the intent is to focus on making steady progress so that overall you'll end up doing enough to make it count. It's all about steadily improving process and capability maturity while effectively protecting payment card data across your control environment.

Example: Create an objective to improve the processes and documentation for a specific percentage of PCI DSS controls each week.

Average output

The second way is to commit sufficient resources to your PCI security program to target the average output. Set a goal and objectives that require higher performance. You may not achieve them all the time, but if you reach them enough, you'll end up making a big difference.

Examples: Improve the daily log-monitoring capability and process. Increase the daily target of the manual log-review processing throughput, and reduce the number of false-positive log alerts so the team can fully meet the intent of PCI DSS Key Requirement 10.

Maximum output

There are several situations that mandate high performance and increased workload for security and compliance initiatives to succeed. That means investing resources and energy to drive maximum output, surmounting a specific, intense threshold that will push your compliance program output to a new level. Examples include driving progress on compliance initiatives with tight deadlines; reorganizing your resources and their assignments and priorities to focus on the PCI security compliance program deliverables, with minimum distraction from work that's not PCI-security related, increasing the input and support received from other departments to maximum capabilities.

When should you target the minimum?

Focusing on the minimum without consistently sustaining the effort is not a recommended strategy for anyone protecting payment card data. Minimum targeting is the art of patience and endurance. When improvements are applied consistently each week, even small efforts can accumulate into large gains over time.

When should you target the average?

Average targeting is the strategy of continuing what you have been doing, but expecting more from yourself, your security teams and your organization—and continuing the effort for longer. In contrast to minimums, many data security and compliance goals are set to try to provoke an average investment. The difference between this approach and a minimum isn't, however, strictly about how much effort you invest. Rather it's about how you frame the goal. Targeting the average is about keeping the long term in mind. You're hoping to sustain something, even if it's not always an easy and consistent output.

When should you focus on the maximum?

Focusing on the maximum has the advantage of expanding the potential of your security and compliance capability. Many areas where growth is needed to improve data security and compliance within your control environment exhibit elements of friction that, barring some kind of intense effort, planning and potential frustration, won't be realized.

> "If you set your bar at 'amazing,' it's awfully difficult to start."[70]
>
> —Seth Godin

The downside of focusing on a maximum is that it often isn't sustainable unless you have proportional investment and commitment from the organization. Bursts of high intensity rarely make for stable, long-term habits.[71]

Maximum targeting should not be applied as a sprint; data security is a marathon. A sprint cannot be sustained perpetually. However, maximum targeting works well when there is an efficiency gain for reaching higher levels of intensity, or when other barriers impede progress without such intensity. For example, if there are critical PCI DSS controls that are not in place, and they are putting your control environment and payment card data at risk, you may need to apply maximum targeting (as a sprint) to break through and overcome constraints that prevent you from putting those controls in place.

Manage goal competition.

Organizations have security and compliance goals that they need to accomplish in the long term. However, many find it difficult to focus on all of them simultaneously.

"Goal competition," where goals are competing with one another for time and attention, is one of the greatest barriers to securing needed commitments and resources. In many organizations, it's common for departments and individuals to pursue multiple goals. In that scenario, the importance of a goal can shift during the year, becoming, for whatever reason, a lower priority compared to a competing one. This can result in key stakeholders or departments investing few resources (attention, time, people, focus, money) in what was originally a prioritized goal, and more in one that's perhaps less critical.

For this reason, it's important to eliminate competing goals and then prioritize those that are remaining. Align your teams and focus your resources into accomplishing your reduced set of prioritized goals before moving on to others.

At the same time, in complex environments like payment card data environments, it's essential to pursue several goals at once.

Contradictory goals are the rule, not the exception. For example, an important goal is to achieve sustainable control effectiveness. PCI DSS requirements have three major goals:

- **Meet all relevant requirements:** the intent of the control objective, the requirements and test procedures
- **Control environment effectiveness:** the intent and objective over extended, uninterrupted periods
- **Control environment sustainability:** sufficient robustness (resistance to unwanted change) and resilience (ability to rapidly recover from unwanted change)

It's essential that all mandatory requirements are met. Compliance with PCI DSS is binary—you either met all of the requirements or you didn't. It's not only the effectiveness of individual security controls, but also the effectiveness of all the interdependent control systems within the environment, that determine the overall effectiveness. To make the control environment more effective, organizations need to do more work, such as improving processes and documentation. This typically requires manual labor, which increases workloads. Increased workloads can divert attention away from other important activities. So, attending to security governance and maturity improvement can, in the short term, be perceived as making the environment less sustainable unless more resources are added. Therefore, it can be perceived that these goals are at odds with each other.

When dealing with problems in complex systems, few activities are as important as setting useful goals. When you don't formulate your goals well or understand their interactions, the performance of the compliance and control environments suffer. If you overlook implicit contradictions among the security and compliance goals, you may initially achieve good results, but in the long run, you'll experience bad results.[72]

[70] "Seth Godin Quotes," https://citatis.com/a20730/26d453

[71] Scott H. Young, "Should You Target the Minimum?" Scott H. Young blog, Feb 2019, https://www.scotthyoung.com/blog/2019/02/13/min-avg-max

[72] "The Importance of Setting Business Goals," happierco, https://www.happierco.com/blog/importance-business-goals/

Security and compliance benefits of clearly defined goals

Clearly articulating and documenting security and compliance goals may be seen as additional work. But there are compelling reasons why it's beneficial to invest the time.

1 **Setting goals helps you establish perspective and frame your approach.**
When you have clearly stated goals (which should be written and communicated to all stakeholders), attention is brought back to what you are trying to accomplish. The 2020 PSR (page 21)[73] included the challenges of security teams being much too focused on technology. "Shiny Object Syndrome" is common. To address this problem, your goals should focus on the achievement of sustainable control effectiveness of the entire control environment, which requires a strategic approach.

2 **Articulating goals helps to focus attention.**
Goals provide decision support. They give you a clear sense of when to say "yes" or "no" to requests that compete for your attention. Strategy is about directing resources to focus on prioritized objectives and goals. It's more about saying "no" to avoid distractions than about saying "yes" and diverting attention elsewhere.

When CISOs and their teams are approached to give away their time and attention, each request can be measured against the stated goals. You can ask yourself, "Does this move me closer or further away from my goals?" We are all busy. The question is: "What are you busy doing?"

3 **Goals allow you to measure overall progress.**
Measuring overall progress is probably one of the most important reasons for having goals and setting milestones and time frames. It presents a yardstick to gauge how you are doing against the overall targeted outcome. Rather than having a vague notion of how the improvement of the control environment is advancing, you have something to measure against.

The security team should work toward goals that result in an organization's capabilities and processes, where the control is sufficiently robust and resilient; where it can confidently and demonstrably be proven that it achieved the required level of sustainable control effectiveness.

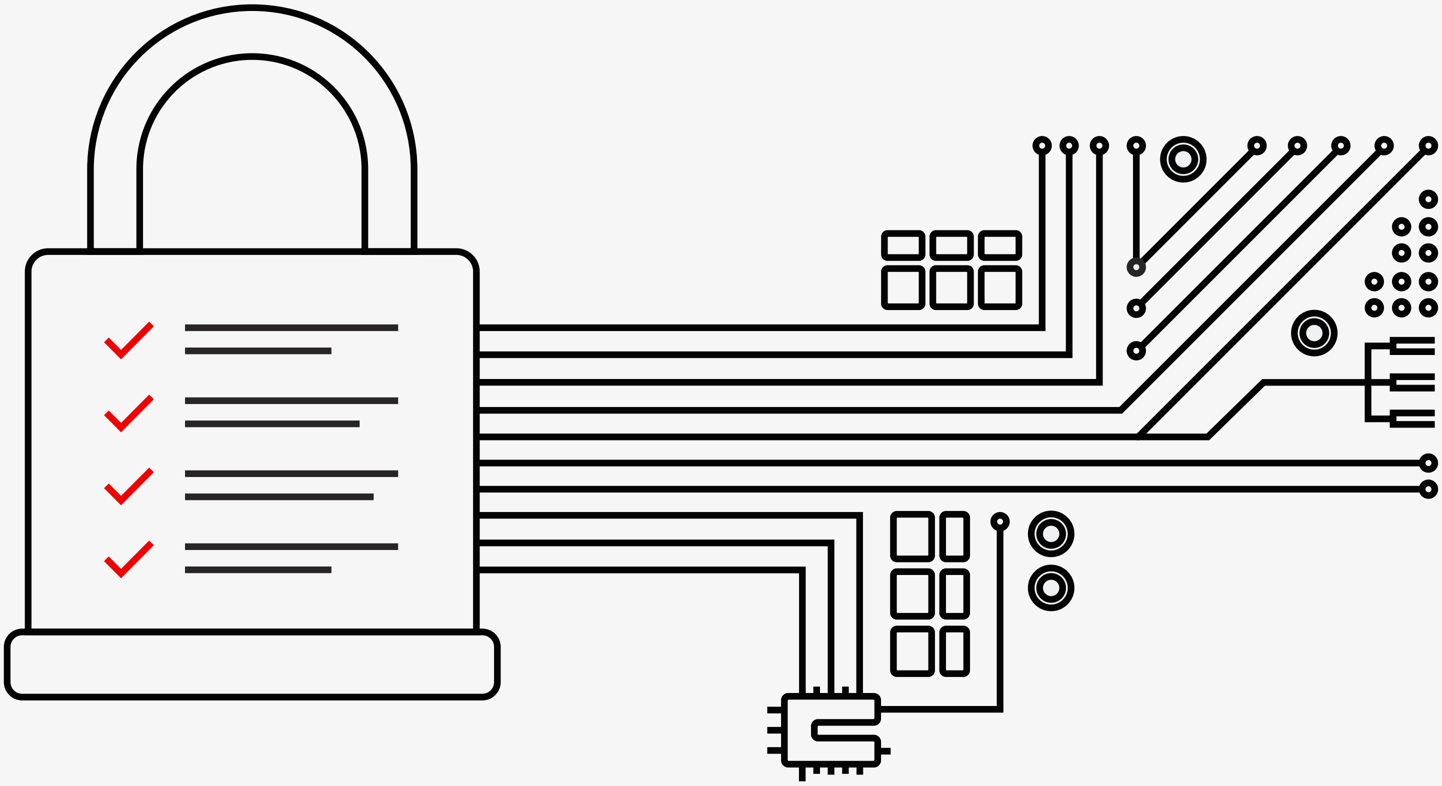
Having these measurements also can give you a sense of accomplishment. Having documented where you started from, it's possible to see your progress. It can keep the motivation of the security team high when working toward a goal becomes hard. From here you can assess what's working, what's not, where you may need some help or how you need to tweak the goal.

4 **Goals should be communicated to employees, contractors, partners and vendors.**
If the goal is vague ("to be PCI security compliant"), not much exists for people to get inspired by nor determine how they can help. Crafted goals and objectives motivate other people to see where they can make a difference for you to achieve your goals. People want to help and contribute, but perhaps don't follow through because they're not clear on how to make an impact. Sharing clear goals and objectives, and why you want to achieve them, helps them understand the organization's needs.

[73] 2020 Payment Security Report, Verizon, 2020, https://www.verizon.com/business/resources/reports/payment-security-report/

Appendix B: Content review and security checklist

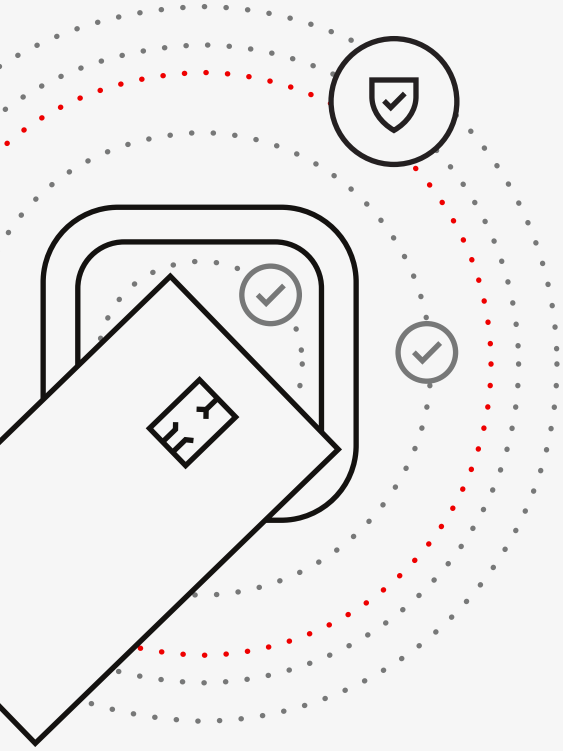
The table on the next page is a summary of essential knowledge and insights gleaned from the Commentary section on page 16. It serves as a handy checklist to help identify which critical elements may not be fully in place within your control environment. During a PCI security assessment, it's common for assessors to find underdeveloped or missing key management elements. This lack of capability and process maturity brings the effectiveness of many, if not most, PCI security programs rightfully into question. The elements listed serve as major milestones on the journey to develop a mature approach to managing governance, risk management and compliance activities.



#	Critical security and compliance management components	Relevance	Yes/No
1	**The Security Management Canvas (TSMC):** Are all five elements of TSMC in place? Review the questions below to decide**.**	Any missing element from TSMC can degrade visibility, management decision-making and performance. See page 32 for details.	
1.1	**Security business model:** Is an up-to-date, overarching security business model applied to support communication and decision-making?	Without a documented business model, it's difficult to clearly express the value of security and compliance, making it harder to secure investment for compliance and security programs.	
1.2	**Security strategy:** Is the strategy effective at directing resources to remain focused on achieving prioritized goals and objectives?	Unclear strategy results in a lack of direction, alignment, focus and clarity on goal and objective prioritization, and muddies the determined path and approach to their achievement.	
1.3	**Security operating model (SOM):** Are all key operational elements across the control environment and their relations documented and visually mapped?	A SOM is essential for understanding how organization structures and processes deliver value, and it's an essential tool for identifying and diagnosing performance issues.	
1.4	**Security frameworks:** Are supplemental security frameworks fully integrated into your GRC/PCI security program?	The use of additional frameworks supports your security and compliance management system. Refer to page 55 of the 2020 PSR for details.	
1.5	**Security program:** Is your program management maturity sufficient to maintain sustainable control effectiveness?	Maintaining management at a program (not project) level helps to direct and ensure the integration and achievement of long-term goals and objectives.	
2	**GRC:** Is your PCI security program fully integrated within your larger corporate governance, risk management and compliance initiatives?	The synchronized integration of all GRC activities translates into increased efficiency and bottom-line financial benefits for businesses.	
3	**Goals:** Are the goals for your overall security and compliance initiative, and for each individual critical management component, clearly defined, documented and communicated?	Clearly defined and communicated goals are indispensable to effectively directing and managing a security strategy and program. Neglecting to communicate goals and objectives is highly detrimental to program performance and outcomes.	
4	**Requirements:** Are all requirements (conditions) to achieve the goals known, fully understood, clearly defined and communicated?	Determining the exact requirements to achieve goals and objectives is essential and includes clarity and distinction between necessary vs sufficient conditions.	
5	**Constraints:** Do you have an effective process to identify and remove all critical program limitations and restrictions that hamper the achievement of goals?	The best approach for performance, capability and maturity improvement is knowing what the biggest constraint is and an ongoing process to repeatedly remove that constraint.	

Appendix C: 5G and payment security

By Ravi K. Annadanam, 5G and MEC Innovation, Verizon Business Group



The appeal of emerging technologies, such as 5G and edge computing, gained significant momentum when the COVID-19 pandemic exposed the weakest links of the financial services industry. Many financial technology (fintech) companies are seeking to use such technologies to help the industry move forward.

COVID-19-related public health concerns also forced many merchants to open their businesses through digital doors, which accelerated the growth of online commerce. This shift of consumer behavior from in-store to online, as well as a significant increase in contactless payments, is expected to become the new norm and continue in the post-pandemic environment. Some smaller retailers forced to close in the crisis may not ever reopen physically but are seeking a digital future instead. The rapid build-out of omnichannel retail capabilities—which will bridge payments in any environment, physical or digital—is expected to become an essential requirement for all commerce.

More digital and mobile device payments

The finance sector is experiencing a significant increase in the use of mobile devices for customer transactions, especially personal banking. The speed and stability of 5G could enhance this experience as well as provide greater security by enabling consumers to opt into advanced biometric-based identification and verification methods. The financial sector could also allow consumers to opt into geolocation technologies in an effort to more effectively pinpoint fraud.

For customers, 5G can provide highly secure connections for video conferencing with financial professionals and loan counselors. Additionally, connecting a 5G device to a 5G network could unleash revolutionary experiences for consumers. For example, 5G may finally deliver on the promise of "shoppable videos." Have you been in a situation where you see a pair of shoes and want to take a picture, click on it and buy them instantly?

The high bandwidth and low latency that 5G can offer could make these shopping experiences possible through what is called augmented reality and virtual reality (AR/VR). The retail industry could also offer “experiential” purchases, such as buying a vacation package or purchasing a bed and other home furniture through AR/VR. The added depth of understanding could boost buyer confidence and potentially improve conversion rates. Enabling new features for consumers opting into them—such as digital IDs, transaction monitoring and reporting to mobile wallets —could fuel even more growth. 5G and edge computing also could make geotargeted offers for consumers opting into such notifications timelier and more accurate, thanks to faster throughput and higher data volumes. These technologies, as well as secure contactless payments, are expected to increase in demand with companies of all sizes.

As mobile transactions increase in volume, security in a digital identity environment becomes paramount, and fraud prevention for mobile transactions becomes critical.

Fraud prevention, combined with consumer awareness, could change consumer attitudes toward data usage and provide opportunities to use mobile and transaction data with customer consent in other areas, such as contact tracing during pandemics.

To embrace emerging e-commerce trends, financial institutions need to increase the speed and reduce the cost of payment processing and leverage cloud-based infrastructure, automation and AI-driven analytics to enhance user experiences.

In summary, providers of managed 5G networks and security services need to understand the uncertainty and increased pressure the financial services and other industries face while providing the technology fabric to address challenges to:

- Adapt to new social conditions
- Apply 5G and mobile edge computing (MEC) to new capabilities
- Stay cyber resilient

What exactly is 5G?

The 5th generation mobile technology (5G) provides a more-advanced global wireless standard, building on the solutions provided by 1G, 2G, 3G and 4G technologies. 5G is designed to interconnect machines, devices and the Internet of Things (IoT). Its technology can deliver higher multigigabits per second (Gbps) speed, and a more uniform experience for a wider quantity of users through a massive network. 5G’s reliability, peak data speeds, ultralow latency and overall improved performance and efficiency will enable new industries, artificial intelligence (AI) and device-centric industries, and more small and medium businesses to connect in new ways.

5G’s unified, more-capable interface and extended capacity for next-generation user experiences will impact every industry—from payment security to remote healthcare, transportation safety and agriculture.

5G building blocks

First generation—1G
1980s: 1G delivered analog voice.

Second generation—2G
Early 1990s: 2G introduced digital voice (such as Code Division Multiple Access [CDMA]).

Third generation—3G
Early 2000s: 3G brought mobile data (such as CDMA2000).

Fourth generation—4G LTE
2010s: 4G LTE introduced mobile broadband.

Potential impact of 5G on payment card compliance

Financial institutions and merchants will continue to find innovative ways to benefit from 5G-enhanced features, open architecture and MEC technologies. At the same time, security practitioners need to explore how these new innovations might impact the payment card industry (PCI) compliance posture. What unintended consequences might occur as society transitions to greater connectivity through 5G networks? Since we are talking about innovation and the future, we don't have answers to all questions, and in many cases, we don't even know what questions to ask. However, the following are some areas to consider:

Education and learning: Traditionally, the work of PCI compliance and security assessors with wireline and Wi-Fi networks is well understood. It is expected that many services and applications in a PCI security scope will be hosted in public or private MEC environments in the future, which will require everyone to understand how cellular networks work, since 5G and MEC are usually combined to provide maximum benefit.

New data flow paths: Many merchants are already exploring how 5G technologies could prove more beneficial than Wi-Fi in some areas, including retail stores. This creates new data flow paths that would traverse not only the 5G radio network, but also back-end wired networks of 5G service providers. Understanding these new data flow paths will be crucial both for merchants and PCI security assessors.

Compliance status of new cloud service provider (CSP) offerings: Major 5G vendors have started offering 5G MEC services that connect 5G networks with CSPs, including Amazon Web Services (AWS), Azure, Google Cloud and others. It's expected that PCI security applications will be hosted in these new offerings from CSPs, which will require PCI compliance.

Threat monitoring for applications hosted in MEC: Traditional security controls (network segmentation, threat monitoring, integrating into SIEM/SOC, encryption, etc.) will still apply for MEC-enabled applications. This will require working closely with 5G service providers, and in some cases, integrating their services into overall solutions for PCI compliance.

New use cases: It's expected that new innovations will create new use cases that would come under a PCI compliance scope—for example, purchases inside AR/VR applications, and interactive videos, apps and games running in a MEC environment.

IoT devices: The 5G standards create new opportunities for using IoT in all industries, including financial and retail segments. It's expected that more and more organizations will use IoT technologies for financial transactions, which will bring new areas under a PCI compliance scope.

Search for a killer app: Many people are searching for a killer app built on 5G technologies. We don't know yet what that killer app will be, but retail and finance sectors are likely to see significant innovation in the coming years, with new ways of doing business that involve payment card processing.

What security features exist in the 5G standards?

Securing the 5G network is about leveraging new security features that are part of the 3rd Generation Partnership Project (3GPP) standards. Enhanced security, as compared with 4G LTE, is possible, thanks to 3GPP's new trust model and security architecture. The main components of the security architecture are:

- **User equipment (UE):** Includes protecting information that could be used to identify and track a subscriber, preventing attackers from modifying user traffic, and ensuring subscribers only connect to trusted cell sites
- **Radio Access Network (RAN):** Provides secure communications on all RAN interfaces and includes extra protections at places that are vulnerable to physical attacks
- **Core network:** Includes specialized network functions (NFs) and enhanced protections for the new service-based architecture (SBA) that NFs will use to communicate

What are public and private MEC anyway?

Mobile edge computing is an evolution of cloud computing services that brings application hosting out from centralized data centers down to the network edge, or in the case of private MEC, actually on-premises, thus closer to wireless devices or 5G endpoints. Developers can use the same familiar cloud platform services and tools (such as compute, networking and storage) on the MEC platform.

Public MEC is located on the edge network closer to the end users; therefore, it can enable network latency in the 20–30 milliseconds (ms) range instead of requiring data to be processed in the core cloud data centers. The network latency range provided does not include application latency and is a target within the coverage area of 5G Ultra Wideband (UWB). This also provides enhanced security and data sovereignty. By enabling cloud servers to run closer to end points, MEC can help developers reduce latency, enhance reliability and speed local processing. MEC also enables processing to happen in the network, rather than in devices, and this can allow for increased battery life and faster deployment of new applications and services.

Private MEC brings these cloud platform services even closer by physically co-locating them on the customer's premises where data is generated and actioned and thereby providing the lower latency range of (10–20 ms), based on the deployment environment, required for the many critical and latency-sensitive applications. Having a private onsite 5G wireless network coupled with these on-premises compute resources can also enable data sovereignty and enhanced security. It's possible for the 5G network operator to provide full end-to-end installation and management, simplifying the customer's day-to-day operations. Think of it as having the cloud in your back pocket!

Our recommendations?

Verizon expects 5G to revolutionize use cases and applications in the financial services industry, including security and fraud control, as highlighted below.

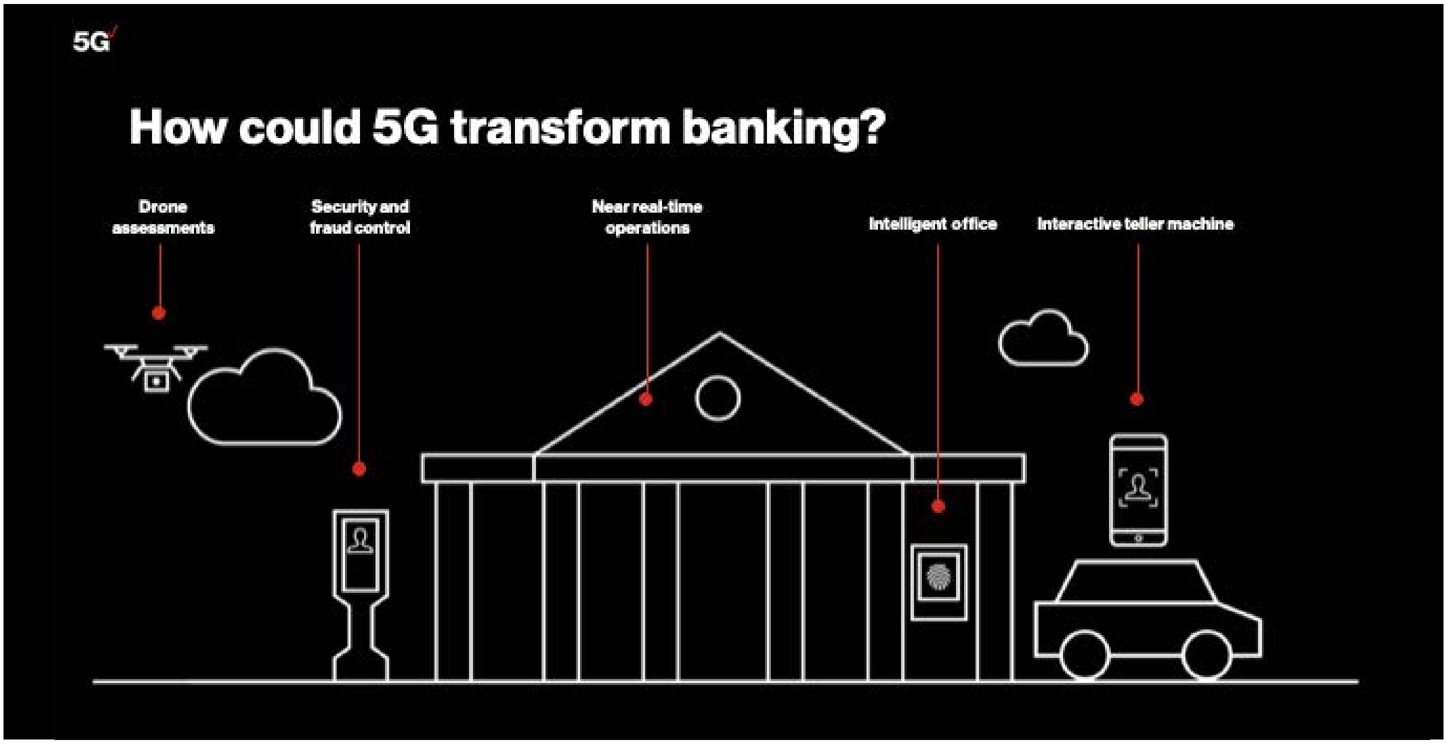

5G
How could 5G transform banking?
Drone assessments
Security and fraud control
Near real-time operations
Intelligent office
Interactive teller machine

Figure 30. Five ways 5G could impact banking

5G use cases in financial services

Security and fraud control

Use case #1

Security challenges that financial services companies face today include:

- Securely monitoring financial transactions
- Assisting customers with wrongfully declined transactions and security updates to applications
- Reducing fraud: In 2020, the U.S. Federal Trade Commission (FTC) received more than 2.2 million reports about fraud totaling nearly $3.3 billion in losses[74]

5G could help solve those – and other – challenges by supporting:

- Increased use of AI and machine learning (ML): These technologies provide risk management and customer service benefits. Additionally, AI is recognized for its fraud detection potential. Some 80% of specialists who use AI to detect fraud believe it has the capability to reduce payments fraud[75]
- Enhanced proactive fraud prevention, with near real-time security monitoring
- Rapid sorting of data, such as transaction amount and merchant ID, to reduce fraud detection errors
- Enabling near real-time security enhancements and updates

The security benefits to businesses utilizing 5G-related services include:

- Boosting mobile security with rapid incident detection and fraud monitoring
- Updating and delivering security enhancements in near real time, without customer involvement
- Allowing more data to travel across networks in near real time, helping to augment fraud prevention

[74] Monica Vaca, "The top frauds of 2020," Federal Trade Commission Consumer Information, Feb 4, 2021, https://www.consumer.ftc.gov/blog/2021/02/top-frauds-2020

[75] "Deep Dive: How AI and ML Can Reduce Fraud and Increase Customer Satisfaction," PYMNTS.com, Feb 23, 2021, https://www.pymnts.com/fraud-prevention/2021/ai-ml-fraud-customer-satisfaction/

5G use cases in financial services

Interactive teller machine

Use case #2

Some of the challenges that today's banks are facing include:

- **High cost of buildings:** Bank branches typically cost between $600,000 and $800,000 a year to run[76]
- **Low profitability:** Just slightly more than half (52%) of all branches in the banking industry are achieving acceptable levels of profitability; more than one-quarter (28%) are below breakeven[77]
- **Traditional customer preferences:** Brick-and-mortar locations are still one of the leading sales channels; 30% to 60% of customers prefer doing some of their banking at branches[78]

5G/MEC-enabled interactive teller machines (ITMs) could help solve these—and other—challenges, by enabling banks to:

- Deploy full-fledged banking services in locations where a traditional brick-and-mortar branch isn't practical
- Support functionality generally found only in brick-and-mortar branches
- Enable remote video sessions with a human banker, where more sophisticated solutions are required or a personalized touch is needed
- Help drive sales through highly personalized services using AI-driven analytics

5G may also help enable near real-time financial operations, accelerating trading, loan transactions and other processes. And intelligent branch/smart offices could provide high customer satisfaction, productivity and shareholder value.

5G security is constantly evolving. Updates to various features are expected in 2022. The content presented in this appendix was written in 2021.

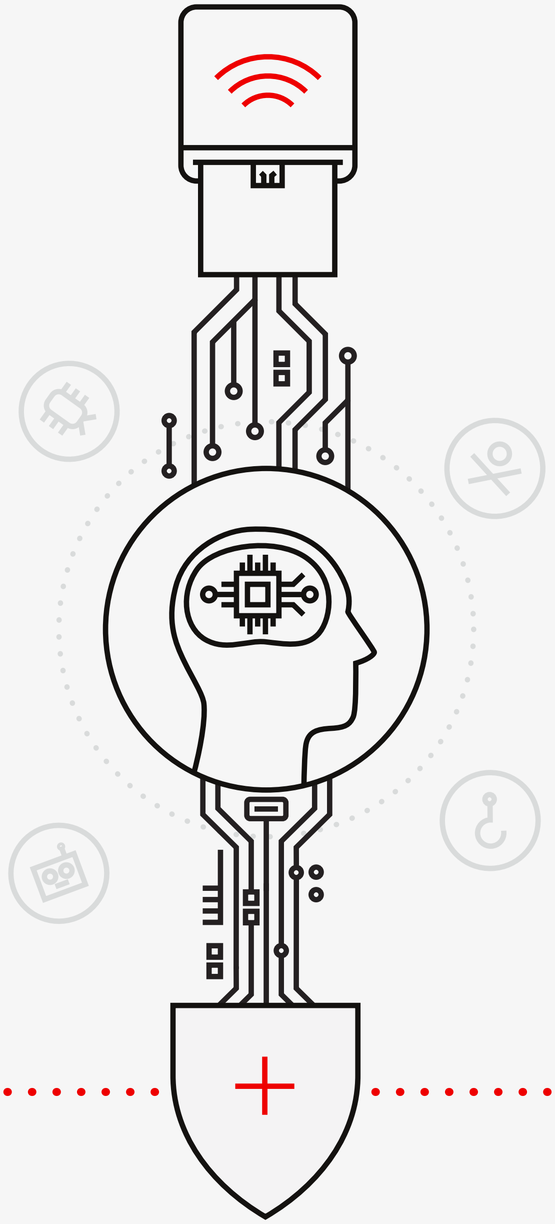
[76] Guenther Hartfeil with Peak Performance Consulting Group, "Are Your Bank's Branches Too Small to Survive?" The Financial Brand, Aug 15, 2018, https://www.thefinancialbrand.com/74386/bank-branch-roi-deposits-profitability/

[77] Ibid.

[78] Klaus Dallerup, et. al., "A bank branch for the digital age," McKinsey & Company, Jul 18, 2018, https://www.mckinsey.com/industries/financial-services/our-insights/a-bank-branch-for-the-digital-age

Appendix D: AI and ML in the payment card industry

By Rafeeq U. Rehman,
Verizon Security Solutions



Machine intelligence is a brave new world that has just started to emerge with significant opportunities for the payment card industry. Effectively managing risk in this new world is crucial to realizing these new opportunities. Expansion of artificial intelligence (AI), especially machine learning (ML), is occurring in a range of areas, including:

- Detecting fraudulent credit card transactions
- Effective targeting for cross-selling and upselling
- Managing credit lines
- Overdraft and pay-later options
- Intelligent chatbots with natural language processing (NLP) capabilities
- Smart and personalized management of reward systems

ML models, if properly built and trained, can identify issues as well as create new opportunities for different players in the payment card industry value chain.

Why organizations should care about advancement in AI/ML

AI clearly is revolutionizing many areas and creating new possibilities, but it also needs careful implementation to safeguard against new types of attacks, such as:

- Poisoning the training or test data to impact ML models' decision-making; embedding backdoors
- Evasion methods that cause a trained model to malfunction
- A variety of other attacks, some of which are listed in the Adversarial Robustness Toolbox documentation[79]

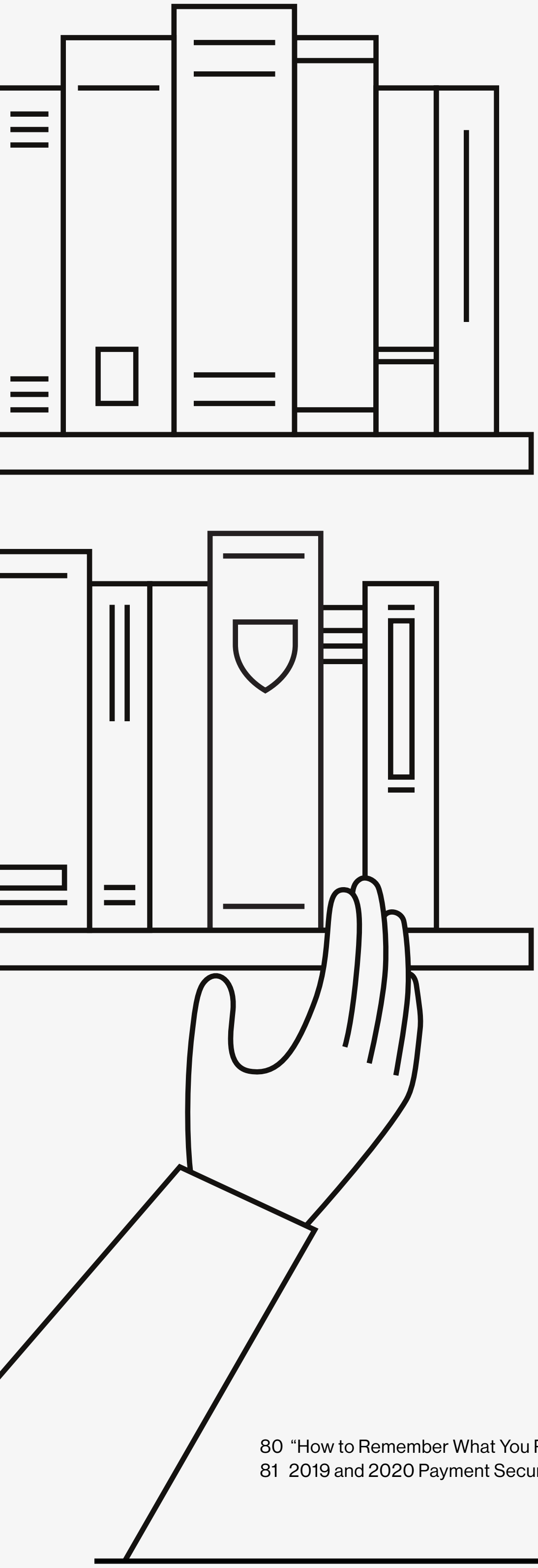
[79] "Art Attacks," GitHub, https://github.com/Trusted-AI/adversarial-robustness-toolbox/wiki/art-attacks

What organizations should consider doing

A major issue for security teams is the lack of understanding of how ML models are built, trained and utilized. Most of this implementation is done by innovation teams that lack a decent understanding of the security implications. So, what should organizations do to prepare for and better understand AI and ML?

Security teams need to create budget and train personnel to build capabilities to understand these new technologies. Organizations need to protect the development and test environment, which is crucial, as this is where models are built, trained and tested. Compromises of these environments are key to poisoning attacks, by altering training and test data sets. This is counterintuitive to the traditional notion of focusing on protecting the production environment. Testing, verification and certification of trained models for vulnerabilities is key to stopping many attacks, especially evasion.

Appendix E: Suggested reading



“Reading alone is not enough. We have to contextualize the knowledge. When does it work? When doesn’t it work? Where can I apply it? What are the key variables? The list goes on. If you can take something you’ve read and apply it immediately, it will reinforce the learning and add context and meaning. Another way to reinforce the learning is to apply the Feynman technique, named after the Nobel Prize-winning physicist Richard Feynman. You can think of it as an algorithm for guaranteed learning. There are four simple steps: choose a concept, teach it to someone unfamiliar with the subject, identify gaps in your understanding and go back to the source material, and review and simplify. Teaching others is a powerful way to embed information in your mind. Upon completing a book, grab the nearest (willing) person and tell them about what you have learned. You’ll have to remove or explain the jargon, describe why this information has meaning, and walk them through the author’s logic. It sounds simple. After you try it the first time, you’ll realize it’s not easy. If there is no one around who is interested, try writing a review where people are encouraged to comment and debate. In order to think for yourself, you need to reflect on your views and see how they stand up to feedback,”[80] according to Farnam Street.

This suggested reading list is a gold mine of information for those tasked with managing security, data protection and compliance programs. One of the best ways to develop proficiency and master data security is to absorb the wealth of information accumulated from experts in the last two decades. CISOs should brush up regularly on guidance from the best and brightest. This list includes new additions to those published in the Verizon 2019 and 2020 Payment Security Reports.[81] This year’s focus is on strategic guidance for CISOs on how to apply a systems approach to complex problem solving and continuous improvement – by using the Logical Thinking Process and the Theory of Constraints to achieve clear goals.

[80] “How to Remember What You Read,” Farnam Street, https://fs.blog/2021/08/remember-books/
[81] 2019 and 2020 Payment Security Reports, Verizon, https://www.verizon.com/business/resources/reports/payment-security-report/

Suggested reading list

	Year	Title	Author	Publisher	Pages	ISBN
1	2007	The Logical Thinking Process: A Systems Approach to Complex Problem Solving (A new edition of Goldratt's Theory of Constraints)	H. William Dettmer	American Society for Quality (ASQ) Press	413	978 0 87389 723 5 https://www.amazon.com/dp/0873897234
2	2020	From Symptoms to Causes: Applying the Logical Thinking Process to an Everyday Problem	Thorsteinn Siglaugsson	Thorsteinn Siglaugsson	54	978 1654 544829 https://www.amazon.com/dp/1654544825
3	1996	Goldratt's Theory of Constraints: A Systems Approach to Continuous Improvement	H. William Dettmer	ASQ Press	378	0 87389 370 0 https://www.amazon.com/dp/B001DORDE8
4	1999	Theory of Constraints	Eliyahu M. Goldratt	North River Press	162	88427 166 8 https://www.amazon.com/dp/0884271668
5	2021	Systems Thinking—And Other Dangerous Habits	H. William Dettmer	Virtual Books	409	978 163838 003 1 https://www.amazon.com/dp/1638680035
6	2010	Theory of Constraints Handbook	James Cox, John Schleier	McGraw-Hill Education	1216	978-0071665544 https://www.amazon.com/dp/0071665544
7	2019	Theory of Constraints, Lean, and Six Sigma Improvement Methodology	Bob Sproull	Productivity Press	306	978-0367247096 https://www.amazon.com/dp/0367247097/
8	1999	Management Dilemmas: The Theory of Constraints Approach to Problem Identification and Solutions	Eli Schragenheim	The St. Lucie Press	208	978 1574 442229 https://www.amazon.com/dp/1574442228
9	1998	Project Management in the Fast Lane: Applying the Theory of Constraints	Robert C. Newbold	CRC Press	284	978-1574441956 https://www.amazon.com/dp/1574441957
10	1999	The Measurement Nightmare: How the Theory of Constraints Can Resolve Conflicting Strategies, Policies, and Measures	Debra Smith	Saint Lucie Press	184	978-1574442465 https://www.amazon.com/dp/B0095H1E0Y
11	1998	Essays on the Theory of Constraints	Eliyahu M. Goldratt	North River Press	280	978-0884271598 https://www.amazon.com/dp/0884271595
12	2003	The Systems Bible: The Beginner's Guide to Systems Large and Small	John Gall	General Systemantics Press	316	978-0961825171 https://www.amazon.com/dp/0961825170
13	1997	Rapid Problem Solving with Post-It® Notes	David Straker	Da Capo Press/ Perseus Books	176	1 55561 142 7 https://www.amazon.com/dp/1555611427
14	2021	Big Breaches: Cybersecurity Lessons for Everyone, 1st ed.	Neil Daswani and Moudy Elbayadi	Apress	474	978 1484266540 https://www.amazon.com/dp/1484266544

September 2022

Verizon 2022 Payment Security Report

Editorial team

Lead author

Ciske van Oosten

Co-authors

Cynthia B. Hanson, Rafeeq U. Rehman, Ravi Annadanam

Lead editor

Cynthia B. Hanson

Data analysts

Abdelkrim Aoued Ahmed Bacha, Allison M. Fortier, Eric Jolent, Mikhail Banguerski, Noel Richards, Ron Tosto, Xavier Michaud

Contributors

Abdelkrim Aoued Ahmed Bacha, Claire Lavelle, Dyana Pearson, Ferdinand Delos Santos, John Galt, John Grim, Michelle Wire, Neal Maguire, Rokon Rokonuzzaman, Sean Sweeney, Virgil Hayes, Xavier Michaud

Payment security consulting practice

Verizon Cyber Security Consulting

Managing Director, Security:
Kristof Philipsen

PCI and payment security consulting practice

Global lead: Sebastien Mazas

APAC region: Ferdinand Delos Santos

Americas region: Matt Arntsen

EMEA region: Loic Breat

Global intelligence: Ciske van Oosten

Legal review: Sudha T. Kantor

Team email:

paymentsecurity@verizon.com

PCI DSS data contributors

Third-party contributors

Marco Borza (Advantio); Héctor Guillermo Martínez, Alberto España, Rogelio Nova, Russell M. Latimer (GMSectec); Anthony Petruso, Michael Vitolo (MegaPlanIT); Ron Tosto (Servadus)

About Verizon Cyber Security Consulting

This research publication is a product of Verizon Cyber Security Consulting, a global leader in the payment security practice with a security team of over 600 consultants in 30 countries. Verizon has one of the largest teams of PCI Qualified Security Assessors.

Verizon is the longest running PCI security services provider in the world, offering services since 2002. Our payment security practice provides PCI and SWIFT consulting, assessments, and program maturity improvement services. Across its Cyber Security Consulting portfolio, Verizon offers services that help clients identify, protect, detect, respond and recover from cyberthreats while ensuring compliance with applicable regulations and standards.