ARMOR

BETWEEN YOU AND THE THREAT

Your PCI 3.1 compliance validation

CISO VANTAGE POINT

KURT HAGERMAN | **CHIEF SECURITY OFFICER | ARMOR**

Tips & guidance to ensure you're ready

Throughout 2014 and 2015, we engaged in deep discussions on PCI 3.0 — the changes it brought to the compliance landscape and the work you need to do to be ready for a successful 2015 audit.

We've conducted webinars, written articles, answered questions and spoken at conferences. PCI compliance is an enormous task and we hope these resources have assisted your organization as you efficiently prepare for your audit.

By evaluating the assessment readiness of your compliance program, you'll identify and correct security gaps, confirm you meet all requirements and prepare for your audit.

"Properly prepare for the audit and you'll feel confident that your organization is in good shape. Remember, compliance is ultimately an essential part of protecting your customers and your brand."

KURT HAGERMAN

Chief Information Security Officer | Armor

Examining CDE

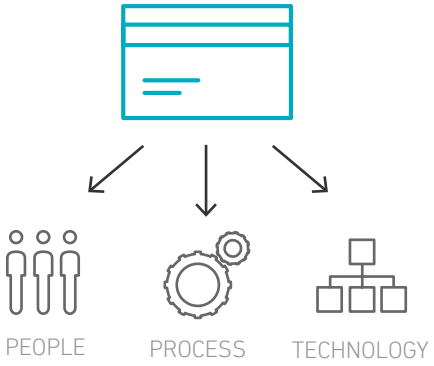
The best place to start: looking at your cardholder data environment (CDE). Ideally, your organization already has a keen focus on defining this area. If you were thorough, you included:

+ All employees who touch cardholder data
+ Processes such as chargebacks, manual orders and reconciliations
+ Inventory of all technology elements, including security services, segmentation systems, virtualization and network components

Check to ensure all relevant elements are defined as being part of your CDE as it is currently — not as it was months ago when you first began your compliance work. This applies to your network and data flow diagrams, so be sure those are accurate.

What is CDE?

Short for cardholder data environment, CDE is the people, processes and technology that store, process or transmit cardholder data or sensitive authentication data.



— PCI Security Standards Council

Drill deeper

Hopefully you've already validated your scoping work by running credit card searches to confirm that your data is in the correct systems.

You're going to run more tests, including another pen test. Remember that this pen test must follow specific 3.1 methods — and you'll need to show the results, too.

In fact, now is the time to review all of the documentation you've collected, including your policies and procedures. Look for more than just diagrams and inventories; your auditor will drill deep into your controls, so be ready to show evidence of strengthened password requirements, new anti-malware tools and other enhanced security measures.

Remember to include your third-party providers, too. Here's a quick reminder: you must have all responsibilities for security, operations, management and reporting spelled out in detailed contracts. This includes any sub-contractors who can impact your environment.

It's not unheard of for an organization to run into audit problems due to a misunderstanding with a provider, so work together to be sure that your division of controls meets 3.1 requirements.

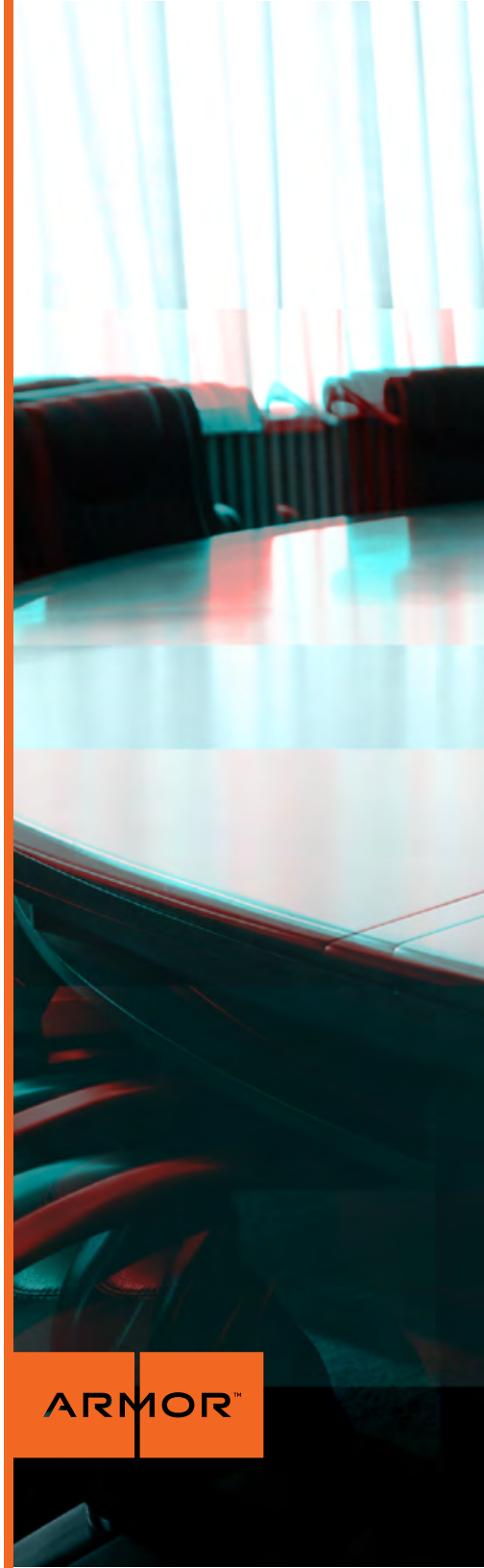
Document compliance

This aligns with the guidance discussed. PCI 3.1 compliance can be complicated, but if there's one aspect that can feel especially time-consuming, it's documentation.

I have some good news, though.

If you've tackled PCI compliance in the past, you may remember that PCI DSS 2.0 wasn't always clear on the kind of documentation needed. Because of this ambiguity, many people — such as auditors, QSAs or security professionals — had questions on just what they had to provide.

Luckily, PCI 3.1 policy includes additional guidance within the revised standards. Instead of simply being told to document something, you'll know what you need to document.



Key PCI 3.1 focus area

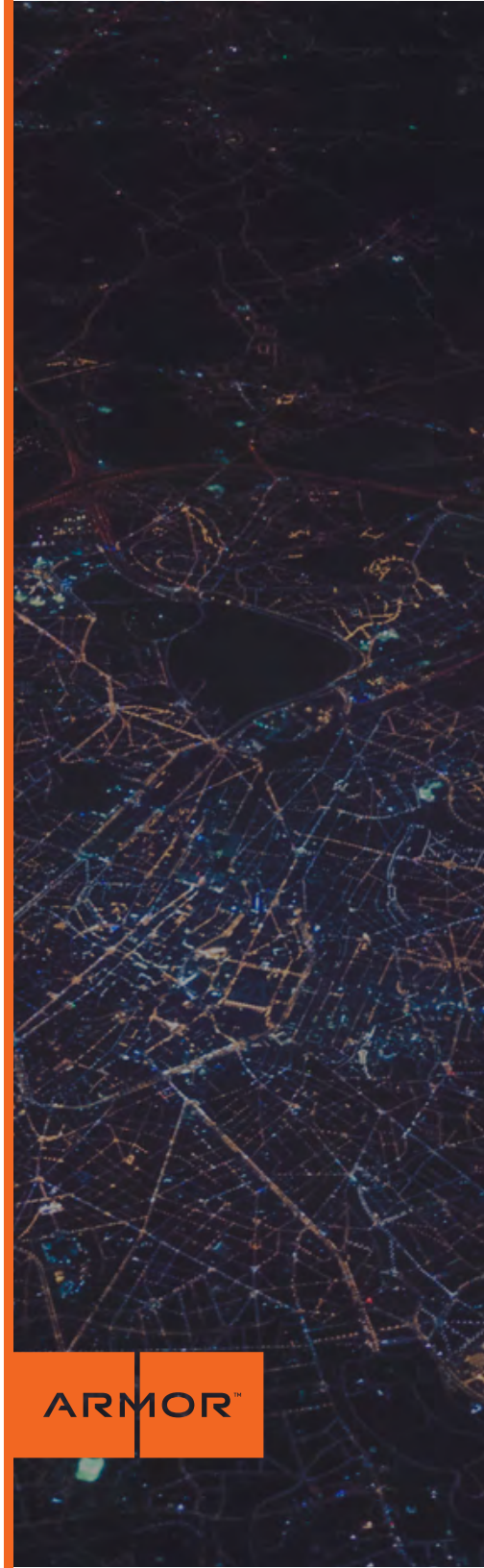
Safe SSL Encryption

The primary driver for the release of PCI 3.1 was the recognition by the Security Standards Council that all versions of the SSL protocol, as well as "early" versions of TLS (most likely only version 1.0, but also some implementations of 1.1), are considered weak forms of encryption.

As a result, PCI Data Security Standard controls (2.2.3, 2.3, 4.1 and 4.1.1) now require that later versions of TLS are used to secure communications after June 30, 2016.

In the interim, if an organization can't eliminate the use of SSL/TLS version 1.0 right away, they must prepare a risk mitigation and migration plan that details how they plan to mitigate risks associated with their use of SSL/TLS version 1.0. This must include the steps they are taking to migrate to a secure version of TLS.

For more information, see the Security Standards Council's April 2015 information supplement titled, "Migrating from SSL and Early TLS."



Key PCI 3.1 focus areas

Data Flows

Having defined and validated your CDE, you'll need to document your work. Provide network diagrams that outline connections and accurate diagrams of your cardholder data flows.

Policies & Procedures

Compliance policies are high-level statements that concern a particular area that align with procedures you implement to carry out those policies. Why does PCI ask for these? They want you to show that you understand the intent of PCI controls and have successfully implemented them within your environment.

Inventories

As you know from defining your CDE, creating an inventory of all relevant components is critical. You'll need to include all security services and segmentation systems, virtualization and network components, and server types. All internal and external applications should be in the mix as well.

You're also required to describe your processes — and their purposes and functions — and all relevant personnel, such as employees, who process cardholder data or have access to cryptographic keys. Finally, remember this isn't a one-time obligation. Your inventory must be accurate at all times.

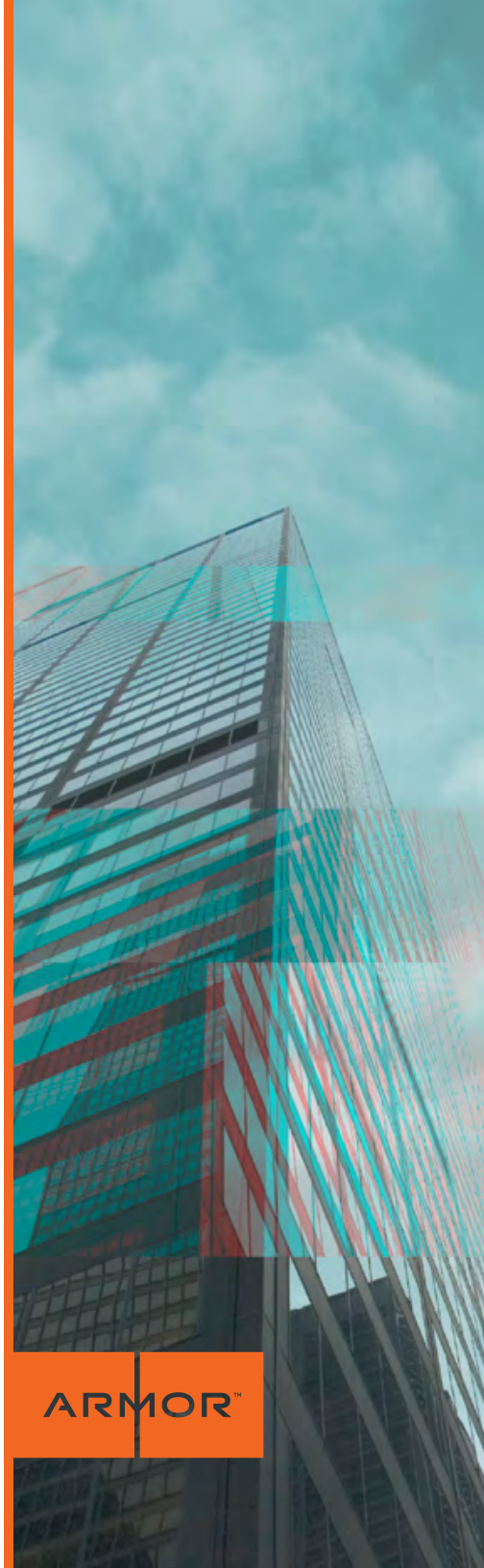
Pen testing

We've talked about the importance of pen testing to ensure your new controls are effective. And, you guessed it. This is something else you'll need to document. Be warned that 3.1 requires you to develop and document a pen-testing methodology that validates your CDE definition and segmentation controls. You also must provide this to the individual conducting your pen test.

Risk Assessments

As you know, risk assessments are absolutely critical. To conduct yours, start by documenting how your organization handles cardholder data, then identify the risks you face.

After you've detailed every kind of threat (e.g., natural disasters, malicious human attacks and environmental threats), assign risk levels to each by assessing the likelihood of those threats occurring and the severity of their impact. Assess the number of people impacted, the cost of the impact and the impact to your brand reputation. Finally, create and implement risk mitigation strategies.



Prepare for success

Finally, it's wise to physically prepare for the audit. Here's my advice on enjoying a faster, smoother and easier audit: have everything ready beforehand. In all of my years assessing organizations, I only witnessed a single company do this — and it gave them an incredible advantage.

Compile and organize all of your documentation, and know where everything is so you can produce it quickly when asked. It's advisable to collect two or three examples of clear and comprehensive evidence that shows you've met each control.

What this tells the auditor: your organization is mature and practices compliance as a regular part of business. If you can establish this confidence, the auditor will be impressed and likely will move more quickly.

My final word of advice to you is not to dread your audit. PCI compliance may require a certain amount of legwork, but there's no real mystery to it. Properly prepare for the audit and you'll feel confident that your organization is in good shape.

Remember, compliance is ultimately an essential part of protecting your customers and your brand. Give yourself a pat on the back for the hard work you did in preparing for your audit.

Good luck.

> "If your organization is mature and practices compliance as a regular part of business, the auditor will be impressed and likely will move more quickly."

KURT HAGERMAN

Chief Information Security Officer | Armor

About Kurt Hagerman

Hagerman serves as chief information security officer (CISO) for Armor. He is responsible for the governance, risk and compliance for both corporate- and customer-facing security solutions and products. Hagerman leads Armor's information security team, serves as the risk officer and ensures Armor maintains its PCI, HITRUST (HIPAA), ISO 27001 and other certifications.

Hagerman regularly consults with Armor prospects and customers on PCI, HIPAA and financial services regulations to help them understand how these regulations impact their business and how Armor can help them meet their regulatory responsibilities.

Hagerman is an active industry speaker and author on information security topics in the payments and healthcare spaces, as well as cloud security. He holds CISA and CISSP certifications and is an active participant with local chapters of ISACA, CSA and ISSA.

Prior to joining Armor, Hagerman was a managing director and national PCI practice director for Coalfire Systems Inc., a leading IT security GRC company. Hagerman has conducted hundreds of security reviews and audits across a number of industries, including the payment space, healthcare, financial services and higher education.

During his 25-plus years in the field of information technology, he has held a wide number of positions encompassing many IT and security disciplines, including network, systems and security engineering, IT/security auditing and compliance.

US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167

ARMOR™
BETWEEN YOU AND THE THREAT