PCI COMPLIANCE GUIDELINES

Thoroughly Explained

2018

LBMC | INFORMATION SECURITY

www.LBMCInformationSecurity.com

CONTENTS

2 Introduction

3 Chapter 1:
What is PCI DSS? How did it get started, and why is it important?

6 Chapter 2:
How do merchants demonstrate PCI compliance?

9 Chapter 3:
How can businesses assess their compliance readiness?

12 Chapter 4:
How can merchants secure their card data effectively and close compliance gaps?

14 Chapter 5:
How does the Report on Compliance process work, and where is PCI heading in the future?

16 Chapter 6:
PCI Version 3.2.1 – What's New?

21 Conclusion

22 About LBMC Information Security

23 Glossary

INTRODUCTION

If you store, process, or transmit credit card data, your business is subject to the Payment Card Industry Data Security Standards (or PCI DSS), a set of security rules designed to curb costly breaches and thefts across the industry.

There are a lot of myths out there about PCI – and those myths can lead merchants to make costly mistakes. In this guide, we'll explore exactly how the PCI DSS works, why it matters, and how to make compliance as smooth as possible.

CHAPTER 1:

WHAT IS PCI DSS?

The PCI DSS consists of over 300 individual requirements, and every merchant — from mom and pop soda shops to big- name chain retailers — must abide by every single one of those requirements. But many merchants misunderstand the rules: how they work, who enforces them, and why they matter in the first place. In fact, it might surprise you to learn the many types of organizations to whom PCI applies. PCI also applies to service providers. The PCI Council defines a service provider as: a business entity that is not a payment brand that is directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data.

So the first step in compliance is clearing up any confusion as to whether or not PCI applies to your organization, and, if so, how it applies.

What is the PCI DSS, exactly, and what makes it so important?

STANDARD ORIGINS

In the early years of the 21st century, the major credit card brands faced a rising tide of fraud for which they held primary liability. Consumers were liable to card issuers for up to fifty dollars, but the brands were responsible for any further fraudulent charges — and this was becoming a significant expense.

The major card brands decided to compel change at the merchant-level by creating standard security rules to prevent thefts both physical and digital. Initially, each of the card brands implemented their own (sometimes inconsistent) sets of rules, including:

- ✓ The Visa Cardholder Information Security Program (CISP)
- ✓ The MasterCard Site Data Protection (SDP)
- ✓ The American Express Data Security Operating Policy (DSOP)

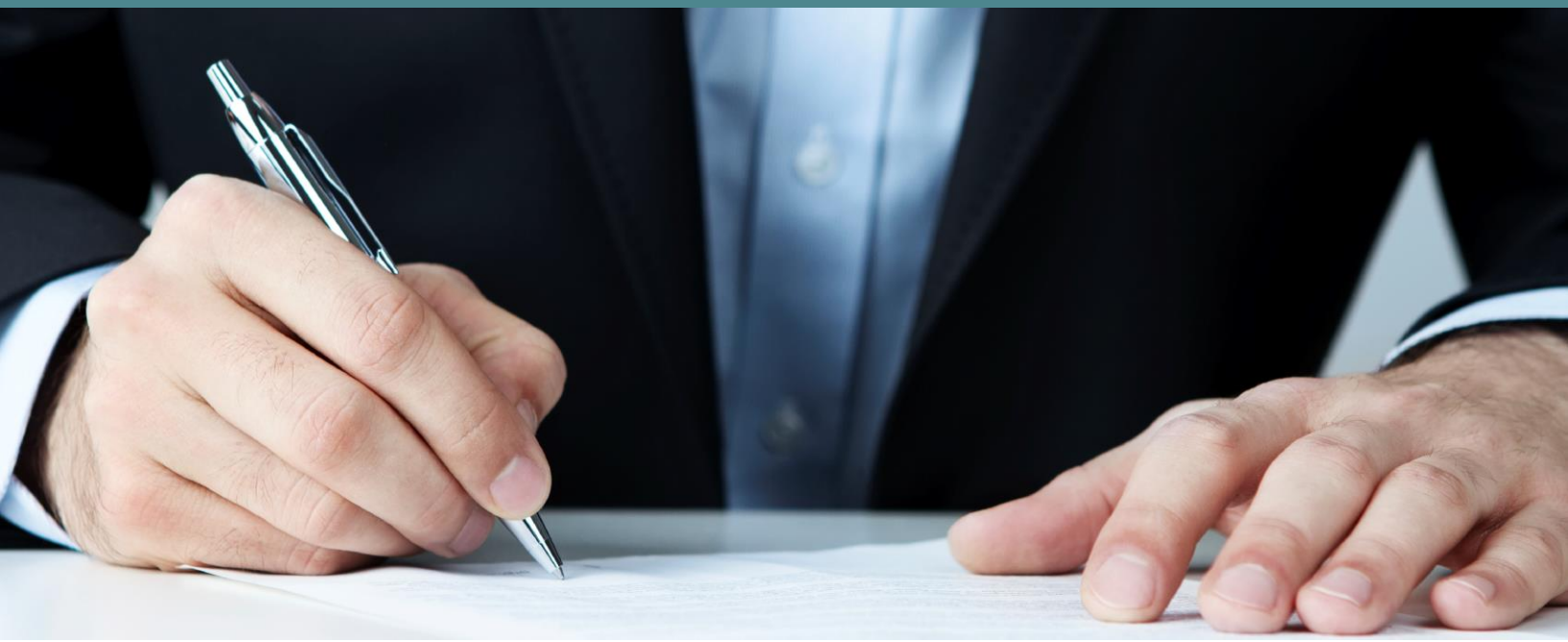
Just keeping the acronyms and abbreviations straight could be a challenge! Unsurprisingly, the different sets of rules created a confusing tangle of compliance requirements for merchants. So in 2004, the card brands worked together to create a single information security standard: the PCI DSS. In 2006, the brands all pitched in to create the PCI Security Standards Council, an independent entity charged with developing, managing, and educating merchants and banks on the standards.

And that brings us to the next key piece of the standards puzzle: the acquiring banks (or "acquirers"), charged with ensuring compliance with the PCI DSS.

MANAGING RISK

The PCI Security Standards Council doesn't fine non-compliant merchants. In fact, it isn't responsible for merchant compliance at all – the Council simply issues and updates the PCI standards on a regular basis. Many companies believe that the card brands themselves assess the fines for non-compliance, but in fact, the card brands hold acquiring banks responsible for their merchants' compliance — and those banks, in turn, may assess fines on merchants at their discretion. As a result, different banks may choose to enforce the PCI DSS differently, though the PCI Security Standards lay out certain reporting requirements based on a merchant's card volume. We'll cover those in greater depth in Chapter 2.

It's natural for many merchants to view the PCI DSS as a chore to be checked off as quickly as possible. While this approach may fulfill the requirements on a superficial level, it misses the underlying opportunity to reduce risk more effectively and gain the most benefit from the investments made in security controls and protections. Today, the PCI DSS can be most constructively described as an evolving set of best practices for security.



The best reason to put security standards in place is because you have performed risk assessments and set out to reduce your risk to an acceptable level, managing risk for its own sake. By approaching the PCI DSS in the spirit of best security practices, you can use it as expert guidance on security for your business and your consumers.

In the following chapters, we'll show you how to do just that.

"The best reason to put security standards in place is because you have performed risk assessments and set out to reduce your risk to an acceptable level, managing risk for its own sake ."

CHAPTER 2:
DEMONSTRATING PCI COMPLIANCE

The PCI Security Standards identify four merchant levels, based on the number of credit card transactions you process.

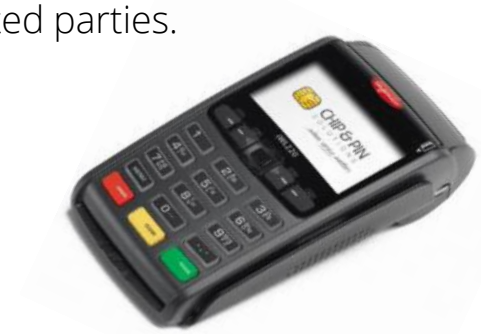
Understandably, many merchants initially worry and wonder about which level applies to them. But the fact is, it doesn't really matter which merchant level you fall under, at least on a practical level, because merchants must comply with all of the PCI requirements regardless of their merchant level. All that matters is the reporting style your acquiring bank requires.

SAQ OR ROC

The term acquiring bank (also acquirer, or merchant bank) is used to refer to the bank that processes credit card transactions on behalf of a merchant. At minimum, an acquiring bank will expect any merchant to fill out a self-reporting questionnaire, called the Self-Assessment Questionnaire (SAQ), on an annual basis. This information is what the PCI Standards themselves require of Level 2, 3, and 4 merchants, which includes the vast majority of businesses.

This questionnaire includes yes-or-no questions corresponding to all 300+ PCI compliance regulations. A merchant must answer "yes" or "not applicable" to every single question to be in compliance. In the event of a breach, both merchant and acquirer will have to hope the questionnaire has been filled out correctly; otherwise, they may still be subject to fines. Mistaken answers, made in good faith, are unfortunately common.

Some acquirers require more exacting reporting — specifically, a formal Report on Compliance (or RoC) from a certified auditor. The PCI Security Standards Council certifies third-party security firms as Qualified Security Assessors (QSAs), which is what we are at LBMC. We help merchants verify that they are in genuine and complete compliance, and we help them report that compliance to acquiring banks and other interested parties.



As far as the PCI Security Standards are concerned, only Level 1 merchants (typically big-name chain retailers) have to submit their Report on Compliance to demonstrate their compliance status. But many acquirers require a RoC for smaller merchants, depending on risk and other circumstances.

For acquirers, RoCs can limit risk considerably, because a RoC represents a third party's validation of your PCI compliance status, and many banks take advantage of the opportunity to require that independent validation of your security posture. This is why determining your merchant level can be a bit beside the point: what you'll need to do depends entirely on your acquirer's expectations, which may be more stringent than your level dictates. If you're choosing an acquirer, it's wise to find out what they expect for PCI compliance right up-front.

GETTING YOUR BASES COVERED

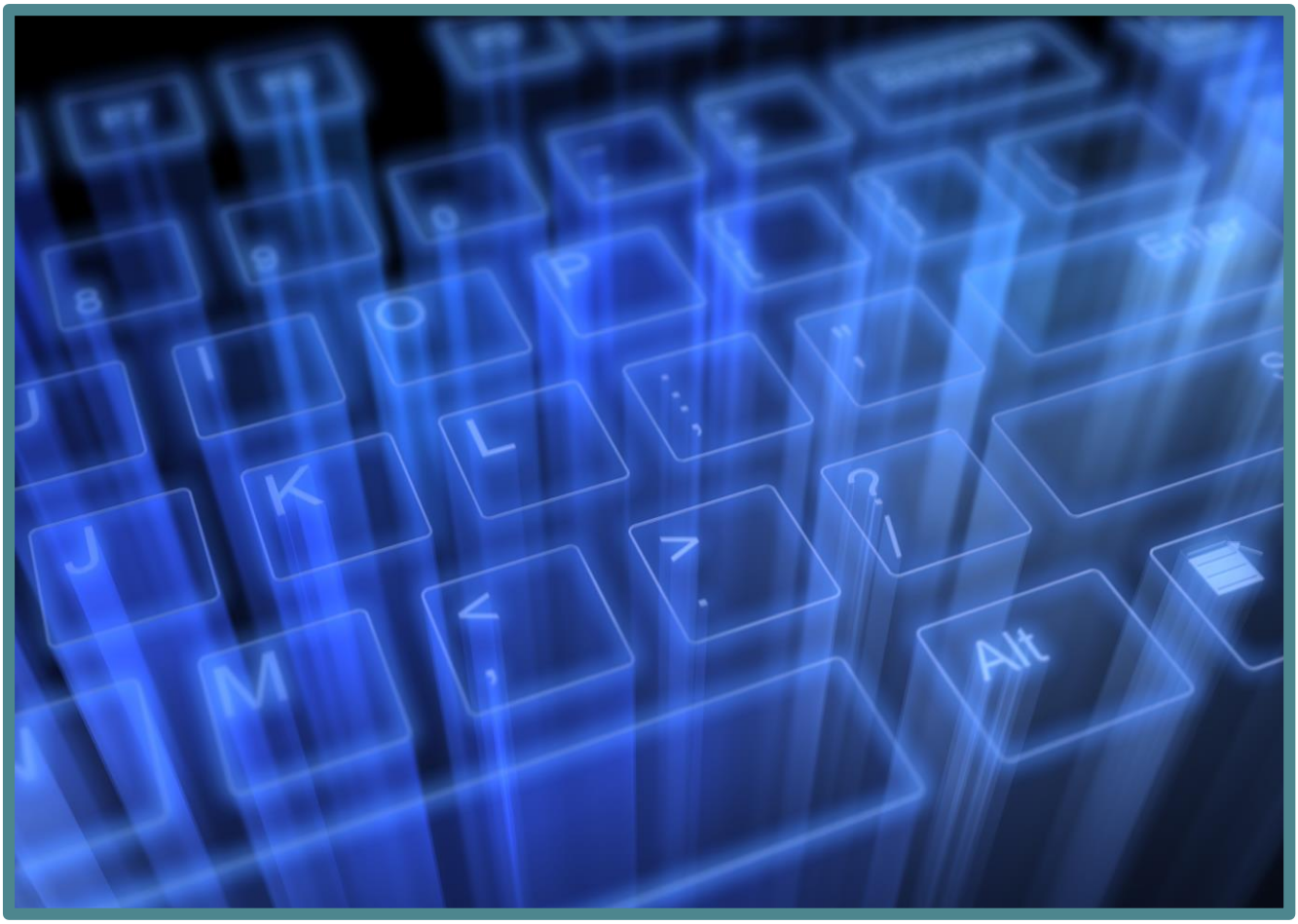
Now we've got a comprehensive picture of all the players involved in PCI compliance regulations: The PCI Security Standards Council, backed by the major card brands, maintains evolving rules, which acquiring banks enforce upon their merchants. Acquiring banks require either a Self-Assessment Questionnaire or a Report on Compliance, the latter of which is supplied by a Qualified Security Assessor. Acquirers may be fined for out-of-compliance merchants, and may in turn assess fines to the merchant. If a security breach occurs at an out-of-compliance merchant, there are also penalties assessed to the acquirer, which will likely be passed on the merchant as well.

It's worth noting that at no point does the government enter the equation. You won't go to jail for non-compliance with PCI. (If you repeatedly flout the rules, you can lose the ability to accept credit cards.) PCI isn't a law — it's an industry-created,

industry-maintained, and industry-enforced set of regulations. In fact, it's more granular and prescriptive than comparable government standards like HIPAA.

Merchants, acquirers, and security experts help to move the guidelines forward, so as time goes on, once-hazy requirements are clarified. It's important to keep up with the PCI requirements regularly to ensure you are meeting any new or recently clarified control areas. Whether you're self-assessing or engaging a QSA, the guidelines can ensure that your data security bases are covered.

So how do you start a compliance assessment? In the next chapter, we'll run through the steps.



CHAPTER 3:
PCI READINESS ASSESSMENT

How can businesses go about making a thorough assessment of their compliance posture?

Even if you've already completed a self-assessment questionnaire, even if you believe in your heart of hearts that you're compliant, it's wise to have PCI security experts perform a readiness assessment at least once. This process will help you verify that you've read the PCI DSS rules correctly and that your assumptions are indeed correct.

It is common for merchants to misinterpret language and mistakenly indicate compliance. A readiness assessment can help you self-evaluate more confidently in the future and help you learn more about how and why your security measures work, as well as identify when they don't work. Often, the assessment reveals opportunities to manage your security more robustly and cost-effectively in the future.

THREE STEPS TO READINESS

What, then, does a typical readiness assessment entail? It consists of three steps:

1: Figure out where cardholder data is stored, processed, or transmitted in your environment.

Where in your business process is credit card data captured, and how is it handled? An assessor will follow the flow of card data through your network, whether it travels to a database or a third-party site. They'll also conduct a thorough search for card data in unexpected places: stored in a spreadsheet in your file-sharing system, or hanging out on your email system, for example.

2: Define the scope for PCI Compliance.

Everywhere card data goes, PCI DSS is the rule of the land. But the opposite is also true: PCI doesn't care about systems that don't have a security impact on credit card data or systems.

So once you've followed the data, you can identify which systems are subject to DSS rules — and which ones you don't need to worry about, at least as far as compliance is concerned. This information may guide your action plan, which we'll discuss in the next chapter, helping you save both time and money.

3: Identify Gaps between your scope and the requirements.

Once you know exactly which portion of your system is subject to PCI DSS, you can compare the rules to the reality. In a readiness assessment, this will typically mean a series of interviews, inspections, and process walkthroughs, validating that all the necessary rules are in place.

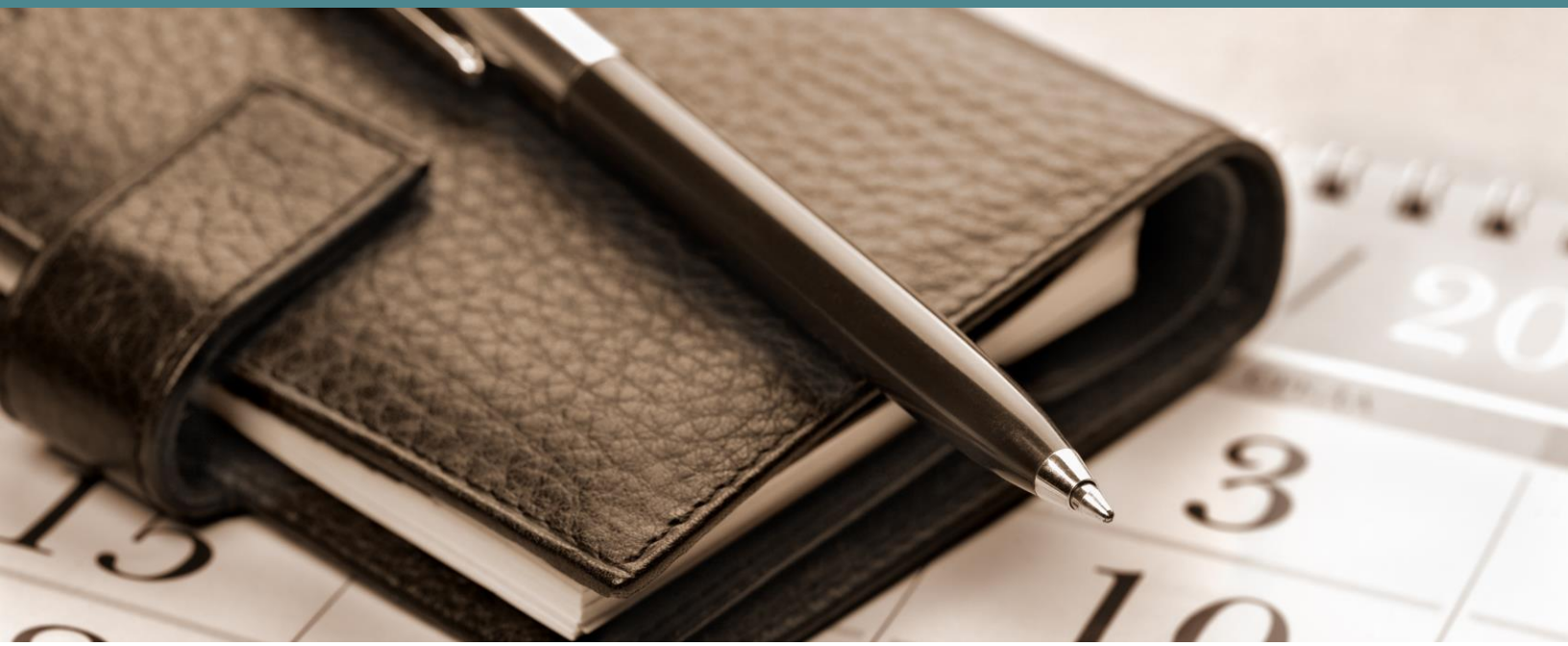
AVOIDING THE PITFALLS

When we perform readiness assessments at LBMC, we see certain problems crop up again and again.

For example, PCI requires businesses to conduct quarterly internal vulnerability assessments — this means scanning for missing patches, default passwords, and other cracks in the armor that thieves or malware could easily exploit. When you find a weakness, you're required to review and remediate results tagged as high-risk. Then you're supposed to run another scan that shows the problem has been addressed.

Often, merchants run the scan but don't read it. Or if they read it, they don't clean up the problem. Or if they clean up the problem, they don't run the scan again — and they don't document the success. For every PCI rule (or "control"), you must have documentation to be considered in compliance. This is an easy and common rule to fall down on.

So we sit down with merchants and look at their past scans, as well as their documentation.



Then we complete the Self-Assessment Questionnaire with them to identify the true answers to every question. This helps them accurately and confidently answer "yes" on each control.

But what about those times when a merchant has to close a gap? What strategies can they use to take action? We'll explore some effective solutions in Chapter 4.

"When you find a technical security weakness, you're required to review and remediate results tagged as high-risk. Then you're supposed to run another scan that shows the problem has been addressed."

CHAPTER 4:
AN ACTION PLAN TO CLOSE GAPS

If you've performed an assessment and determined that you're not in compliance, you know that you're at heightened risk of breach and penalty.

So what steps can you take to secure your data effectively without breaking the bank?

WEIGHING RISK

If your gap assessment was performed properly, it will have identified your highest risk areas. Naturally, you'll want to address these first, prioritizing vulnerabilities that pose the most danger, exposing your card data or systems directly. Ultimately, your goal is to reduce your attack profile and buy yourself time to ensure that you've completely addressed your security risks.

What is the difference between a high-risk and low-risk vulnerability? If a merchant stores a card's authorization data (CVV codes or Track Data) after the authorization process is complete, that's an immediate and first-order violation — and it needs to be rectified at once.

By contrast, if you simply lack proper documentation for an otherwise up-to-snuff control...well, that'll need to be addressed, but it can probably wait until you've fried the bigger fish.

COMPLIANCE STRATEGIES

Sometimes, the most effective way to eliminate compliance gaps is to look at the big picture. In Chapter 3, we discussed how PCI rules apply to a certain scope of a merchant's systems: specifically, anywhere that card data travels. Often, only a small number of a business's systems process or store cardholder data, and this creates an opportunity.

To reduce the scope and burden of PCI compliance, you can separate your systems that handle card data from everything else — freeing

everything else from PCI rules. This is sometimes called system and network segmentation. Imagine a physician's office, for example; systems related to building operations may have nothing whatsoever to do with patients' card data, so it won't necessarily make sense to spend the time and money to apply the same security controls that you would with a payment system. Walling off payment systems from everything else may cost less than configuring and enforcing PCI-compliant measures on every system.

Sometimes, however, segmentation simply isn't practical. At that same physician's office, if the vast majority of computers are connected to both building operations systems and payment systems, then segmentation isn't going to make much sense. The usefulness of this approach will depend on the situation.

THIRD-PARTY PARTNERS

Many compliance responsibilities can be transferred to third-party firms. In fact, a Qualified Security Assessor can also provide managed security services or conduct penetration tests, helping you turn your attention to your business. Like segmentation, this is a strategy that should be considered on a case-by-case basis. For example, smaller organizations can often make do with open source software or manual processes, whereas the cost of compliance is often high for large companies because of the sheer scope and number of systems in their cardholder data environment.

It's important to remember that a third party never takes on full responsibility for your compliance. You can't tell your acquirer, "Someone else is handling it." You'll have to coordinate with your partner to ensure that you have an accurate questionnaire or RoC. This should include clearly identifying each party's PCI responsibilities in the contract with your third party, and regularly checking up on their compliance efforts.

Which brings us to our final topic: Streamlining the RoC process. We've seen how self-assessing organizations can approach PCI compliance. But if yours is an organization that requires a Report on Compliance from a QSA, how can you make it run more smoothly?

CHAPTER 5:

PCI AUDIT: STREAMLINING THE REPORT ON COMPLIANCE (ROC) PROCESS

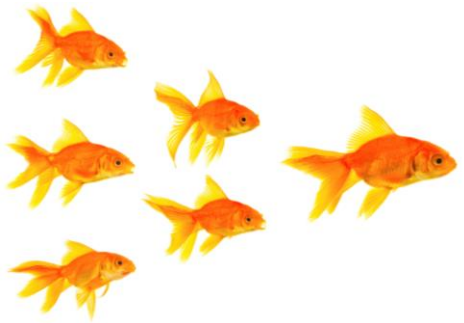
How can businesses streamline the Report on Compliance process? As a Qualified Security Assessor, we've identified a handful of steps that make the process run as smoothly as possible for merchants.

STEPS TO SUCCESS

Typically, a successful RoC process consists of three basic steps:

1: Identify a Collaborative QSA.

For the process to be as efficient as possible, it needs to be a collaborative process. Try to identify and partner with a QSA that demonstrates a solid understanding of your business environment. The QSA should also be able to explain its fieldwork protocol clearly.



2: Get the documents in order.

A Report on Compliance requires documentation for every control — which adds up to quite a lot of documentation indeed. Look for your QSA to give you plenty of time to get the documents together. Four to six weeks is an appropriate amount of lead time.

3: Talk ahead of time.

A QSA should schedule interviews with your key personnel a few weeks before they come on-site, so they can be conscious of your people's time while gathering the data they need. Regular communication is fundamental, so when the QSA identifies areas of noncompliance, you can address it as quickly as possible. As long as an issue is addressed before the QSA writes its report, you should get credit for compliance. Make certain that you have a key internal contact regularly managing potential issues and

handling requests for artifacts or documentation from your QSA so nothing falls through the cracks.

What you don't want in a partner is a QSA that flies out an assessor who spends a few days onsite (or no time at all), never speaking to you before or after. Find a partner who can educate you throughout the process and that is willing to transfer knowledge to your internal team so you can stay on top of PCI in the future. Remember the spirit of PCI DSS is to instill best security practices in your company and help ensure that they become a permanent part of your operations. A good partner can help you strengthen your security and your confidence.

LOOKING FORWARD

As we discussed in Chapter 2, the PCI DSS is an evolving set of standards. Among the most important rules for choosing a QSA is finding an organization that is in tune with the direction of the standards, and can help you prepare for the future — not simply check off the boxes for today. For merchants currently tracking their security measures to today's version of the DSS, it would be wise to identify items they will need to change as new versions are announced. An up-to-date QSA will help you be future-aware.

The overarching trajectory of PCI DSS is to help organizations get to the point where security as a whole, including PCI compliance, is business as usual. The priority shouldn't be getting your acquiring bank off your back — rather, you want a thoughtful security strategy to permeate your organization, managing risk for its own sake.

"Remember, the spirit of PCI DSS is to instill best security practices in your company and help ensure that they become a permanent part of your operations. A good partner can help you strengthen your security and your confidence."

CHAPTER 6:

PCI VERSION 3.2.1 – WHAT'S NEW?

The newest version of the PCI DSS, version 3.2,1, was released in June 2018. It represented a minor update to the last major version update that was released in May 2016 (3.2). After a grace period to allow for the planning and adoption of some of the more rigorous changes from the last major update, the requirements went into full effect on February 1, 2018. You can find the very latest information on PCI compliance directly from the PCI Council: https://www.pcisecuritystandards.org/

Most of the changes in the latest version impose additional security requirements and checkpoints for outside service providers. Service providers often have access to many different organizations' cardholder data systems, and therefore are a good target for attackers. Compromising a single service provider can offer access to cardholder data from many other entities. Many high-profile breaches, such as Home Depot and Target, originated with a third-party service provider. Here are some key changes, with the associated PCI DSS 3.2 reference number:

1: Multi-Factor Authentication – 8.3.1

All merchants and service providers must use multi-factor authentication for all non-console administrative access into the Cardholder Data Environment (CDE). This means that all administrative logins to CDE systems, regardless of whether they occur from outside the network or from an office location on the entity's private network, must use multi-factor authentication for every login. This change will likely require a significant effort from many organizations that have typically utilized multi-factor authentication for remote access only.

2: Change Control Process Validation – 6.6

While technically a new requirement in version 3.2, this specification simply requires that an entity ensure that all changes to in-scope components include all PCI requirements, and that applicable documentation be updated upon completion of the change.

While organizations would have had to complete this activity anyway in order to be PCI compliant, the addition of the control requirement simply formalizes their efforts and serves as a reminder of the need to ensure that all bases are covered when making changes to the CDE.

3: SSL Clarification

Secure Sockets Layer (SSL) and early versions of the Transport Layer Protocol (TLS) encryption protocols are no longer considered secure, and must be removed from use in the PCI CDEs and replaced with current versions. The PCI Council has added an appendix (A2) to the PCI v3.2 documentation. This supplemental information provides clarity about how to address migrations to TLS 1.1 or higher.

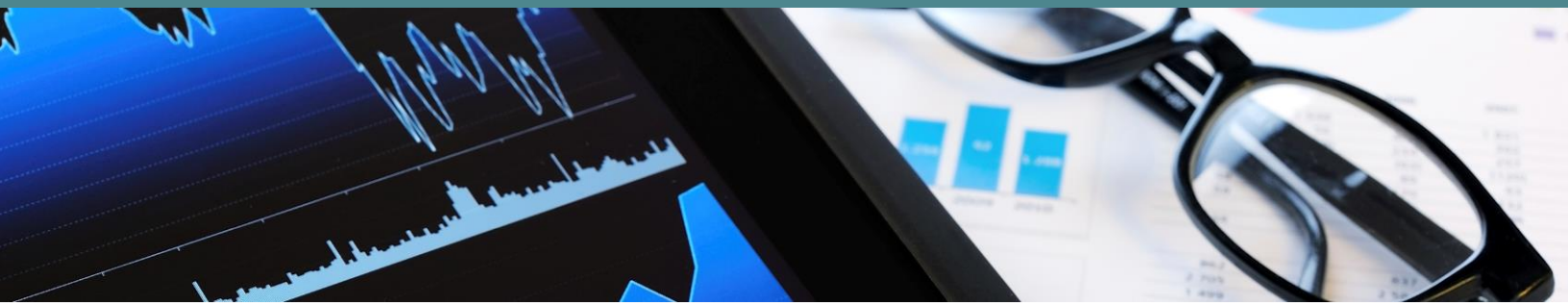
The remaining "evolving requirements" summarized below are applicable to service providers.

4: Reporting Security Control Failures – 10.8.1

Service providers are required to implement a process for the timely detection and internal reporting (not to customers!) of critical security control system failures, including but not limited to:

- ✓ Firewalls and IDS/IPS
- ✓ FIM
- ✓ Anti-virus
- ✓ Physical access controls
- ✓ Logical access controls
- ✓ Audit logging mechanisms
- ✓ Segmentation controls (if used)

This requirement is intended to ensure that security monitoring controls (that were already required to be in place) are functioning as intended and that alerts, notifications, and any instances where the controls did not function as expected are identified and promptly addressed.



5: PCI DSS Penetration Testing to Confirm Scope – 11.3.4.1

If service providers are using a network segmentation strategy, as discussed in Chapter 4, they must confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months, AND after any changes to segmentation controls/methods. This can be done by a qualified internal employee or third party who is experienced in penetration testing.

6: Quarterly Reviews – 12.11

Outside service providers are required to perform reviews at least quarterly to confirm personnel are following established security policies and operational procedures. The reviews must cover the following processes:

- ✓ Daily log reviews
- ✓ Firewall rule-set reviews
- ✓ Applying configuration standards to new systems
- ✓ Responding to security alerts
- ✓ Change management processes

The intent here is for service providers to ensure that PCI DSS becomes "business as usual" in their organizations, and that the execution of control processes is not done simply to satisfy PCI requirements, but rather as a regular operations activity.

7: Security Documentation – 3.5.1

Service providers must keep a documented description of the crypto-architecture used to protect cardholder data. This helps merchants understand how a service provider is encrypting and protecting cardholder data, on their behalf.

8: Executive Management Responsibilities – 12.4.1

Executive management from third parties must establish responsibility for the protection of cardholder data and a PCI DSS compliance program that includes:

- ✓ Overall accountability for maintaining PCI DSS compliance
- ✓ Defining a charter for a PCI DSS compliance program and communication to the service provider's executive management

The intent with this requirement is to ensure that the executive management team of a service provider understands and accepts its responsibility for designing, operating, and maintaining a PCI-compliant service.

SUMMARY OF PCI v3.2.1

The revision was published May 17, 2018. The Council has emphasized that the revision will be minor and that "there will be no new requirements in this revision."

Rather than introducing new requirements, PCI DSS v3.2.1 is intended "remove the effective date introduced in version 3.2 for several new requirements and the Secure Sockets Layer (SSL)/early Transport Layer Security (TLS) migration requirements."

As you may know, there were specific new requirements in version 3.2 that specify an adoption date of February 1, 2018. These dates have now passed and version 3.2.1 simply removes this wording.

In addition to updating the language around these requirements, the revision is intended to "fix minor typographical errors, punctuation, and format issues."

On the whole, PCI DSS v3.2.1 is not a cause for concern. It introduces no new expectations and falls directly in line with the plan set forth in version 3.2.

CONCLUSION

PCI compliance is complex, but with the right risk management approach it can be smoothly integrated in your day-to-day operations and become just another part of doing business.

It's easy for an employee to accidentally create a rogue wireless access point...but that means your network is vulnerable, potentially allowing intruders to steal card data from the parking lot. It's easy to forget to install a patch or perform a regular scan. Both of these activities can also leave you vulnerable.

Once businesses are aware of, monitoring for, and responsive to the full spectrum of cybersecurity threats like these, they'll be prepared to move confidently into the future, secure in the knowledge that they've protected their customers, their data, and themselves.

ABOUT LBMC

While regulatory compliance is mandatory, so is operating a successful business. A well-designed information security program provides critical intelligence about risks facing your business so your executive team can make well-informed decisions.

As a member of the family of LBMC companies, LBMC Information Security separates itself from traditional information security firms by offering practical, cost-effective solutions that are customized to your unique risk environment. We tailor our assessments and deliverables to your organization's risk tolerance, providing the highest level of risk reduction for the associated cost. These practical solutions lead to real results and a tangible return on investment.

PCI DSS COMPLIANCE SERVICES

Our full suite of payments-related data security services helps organizations in every PCI tier achieve compliance today and reduce the risk of non-compliance in the future, including:

- ✓ PCI Readiness Assessment
- ✓ PCI Audit & Report on Compliance
- ✓ PCI Flash Assessment
- ✓ PCI Gap Assessment
- ✓ PCI Consulting (Virtual QSA)
- ✓ PCI Penetration Testing
- ✓ ASV Quarterly Scanning
- ✓ Risk Assessments
- ✓ Web Application Security Pen Testing
- ✓ IDS/IPS Monitoring
- ✓ Cloud-Managed SIEM
- ✓ Card Data Discovery
- ✓ PCI Training & Education

READY TO DISCUSS YOUR NETWORK SECURITY CONCERNS?

Contact us for a free consultation:
www.lbmcinformationsecurity.com/contact-us

GLOSSARY

TERM	DEFINITION
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution". An entity, typically a financial institution, that processes payment card transactions for merchants and is defined by a payment brand as an acquirer.
AOC	Abbreviation for "attestation of compliance." The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance.
ASV	Abbreviation for "Approved Scanning Vendor." An ASV is a company approved by the PCI SSC to conduct external vulnerability scanning services for a merchant or service provider.
Card Skimmer	A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.
Card Verification Code or Value	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features. (1) Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. (2) For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic.

TERM	DEFINITION
CDE	Abbreviation for "cardholder data environment." The CDE consists of the people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data, and all other systems that are connected to the same network.
Compensating Controls	Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must: ✓ Meet the intent and rigor of the original PCI DSS requirement; ✓ Provide a similar level of defense as the original PCI DSS requirement; ✓ Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and ✓ Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.
File Integrity Monitoring (FIM)	Technique or technology under which certain files or logs are monitored to detect if they are modified. When critical files or logs are modified, alerts should be sent to appropriate security personnel.
IDS	Abbreviation for "intrusion-detection system." Software or hardware used to identify and alert on network or system anomalies or intrusion attempts. Composed of: sensors that generate security events; a console to monitor events and alerts and control the sensors; and a central engine that records events logged by the sensors in a database. Uses system of rules to generate alerts in response to detected security events. See IPS:
IPS	Abbreviation for "intrusion prevention system." Beyond an IDS, an IPS takes the additional step of blocking the attempted intrusion.

TERM	DEFINITION
Masking	In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
PAN	Acronym for "primary account number" and also referred to as "account number." Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
Payment Application	In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties.
PCI DSS	Abbreviation for "Payment Card Industry Data Security Standard."
POS	Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.
QSA	Abbreviation for "Qualified Security Assessor." QSAs are qualified by PCI SSC to perform PCI DSS on- site assessments.
RoC	Abbreviation for "Report on Compliance." A report, issued by a PCI QSA, documenting detailed results from an entity's PCI DSS assessment.

TERM	DEFINITION
SAQ	Abbreviation for "Self-Assessment Questionnaire." Reporting tool used to document self-assessment results from an entity's PCI DSS assessment. An SAQ can be completed by the merchant itself or in collaboration with a PCI QSA.
Scoping	Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review.
Sensitive Authentication Data	Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.
Service Provider	A business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).
System Components	Any network devices, servers, computing devices, or applications included in or connected to the cardholder data environment.
Track Data	Also referred to as "full track data" or "magnetic-stripe data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portion of the magnetic stripe.

PCI RESOURCES

Below is a list of additional reference material from LBMC's PCI Security team. Each resource name may be clicked to go directly to the associated web page.

PLANNING FOR COMPLIANCE

- 3 Types of Tasks You Should Document for PCI DSS Compliance
- 7 Keys to Comprehensive PCI DSS Documentation
- Attaining PCI Compliance With Vulnerability Scanning
- 6 Myths About PCI Compliance Regulations
- Five Steps for Maintaining Compliance in the Cloud
- Penetration Testing and PCI Compliance Requirements
- Developing an Effective Security Awareness Program: Physical Security, Password Security, and Phishing

MANAGING PCI COMPLIANCE COSTS AND RISKS

- 3 Ways to Reduce the Costs of PCI Compliance Regulations
- Reducing PCI Scope, What Makes Good Network Segmentation? (Our most popular blog post)
- How to Explain PCI Compliance Penalties to Beginners
- PCI Compliance Fees, Fines, and Penalties - What Happens After a Breach
- Why the Target Settlement Should Make Merchants and Consumers Nervous

PCI'S EVER-CHANGING CHALLENGES

- PCI DSS Version 3.2: What You Need to Know
- PCI Version 3.1 - Changes Coming to SSL
- PCI 3.1 Compliance Deadline is Here
- What Healthcare Organizations Need to Know About PCI 3.1 Compliance for Mobile Payments

PIN-ENTRY DEVICES

- Fast Approaching Deadlines to Ensure Point-of-Sale PIN-Entry Devices are Secure
- How Does EMV Adoption Relate to PCI Compliance?
- PCI Security Standards Council's Approved PIN Transaction Security (PTS) Devices

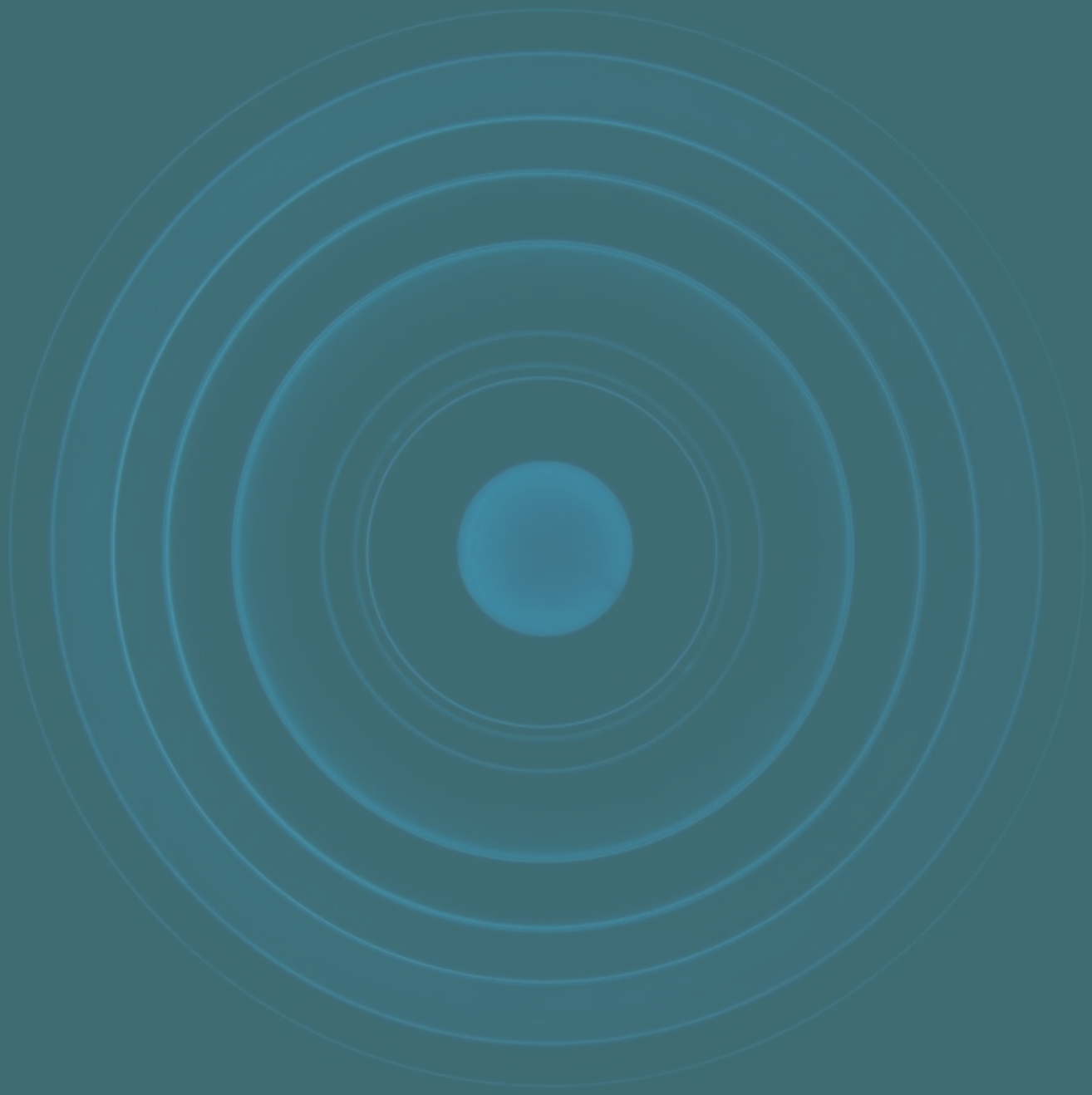
PCI SECURITY STANDARDS COUNCIL RESOURCES

- Document Library - PCI DSS specifications, terms and abbreviations, and much more
- Completing the Self-Assessment Questionnaire
- List of Validated Payment Applications
- Point-to-Point Encryption (P2PE) Solutions
- Point-to-Point Encryption (P2PE) Applications
- Point-to-Point Encryption (P2PE) Components for merchants implementing their own Merchant Managed Solution – MMS

PCI PAYMENT PROTECTION RESOURCES FOR SMALL MERCHANTS

- Guide to Safe Payments
- Common Payment Systems
- Questions to Ask Your Vendors
- Glossary of Payment and Information Security Terms

LBMC | INFORMATION SECURITY



PCI COMPLIANCE GUIDELINES EXPLAINED

Copyright © 2018

Published by LBMC Information Security
Nashville, Knoxville, Chattanooga

All rights reserved. Except as permitted under U.S. Copyright Act of 1976, no part of this publication may be reproduced, distributed, or transmitted in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher. Design by LBMC. Visit our website at www.LBMCInformationSecurity.com