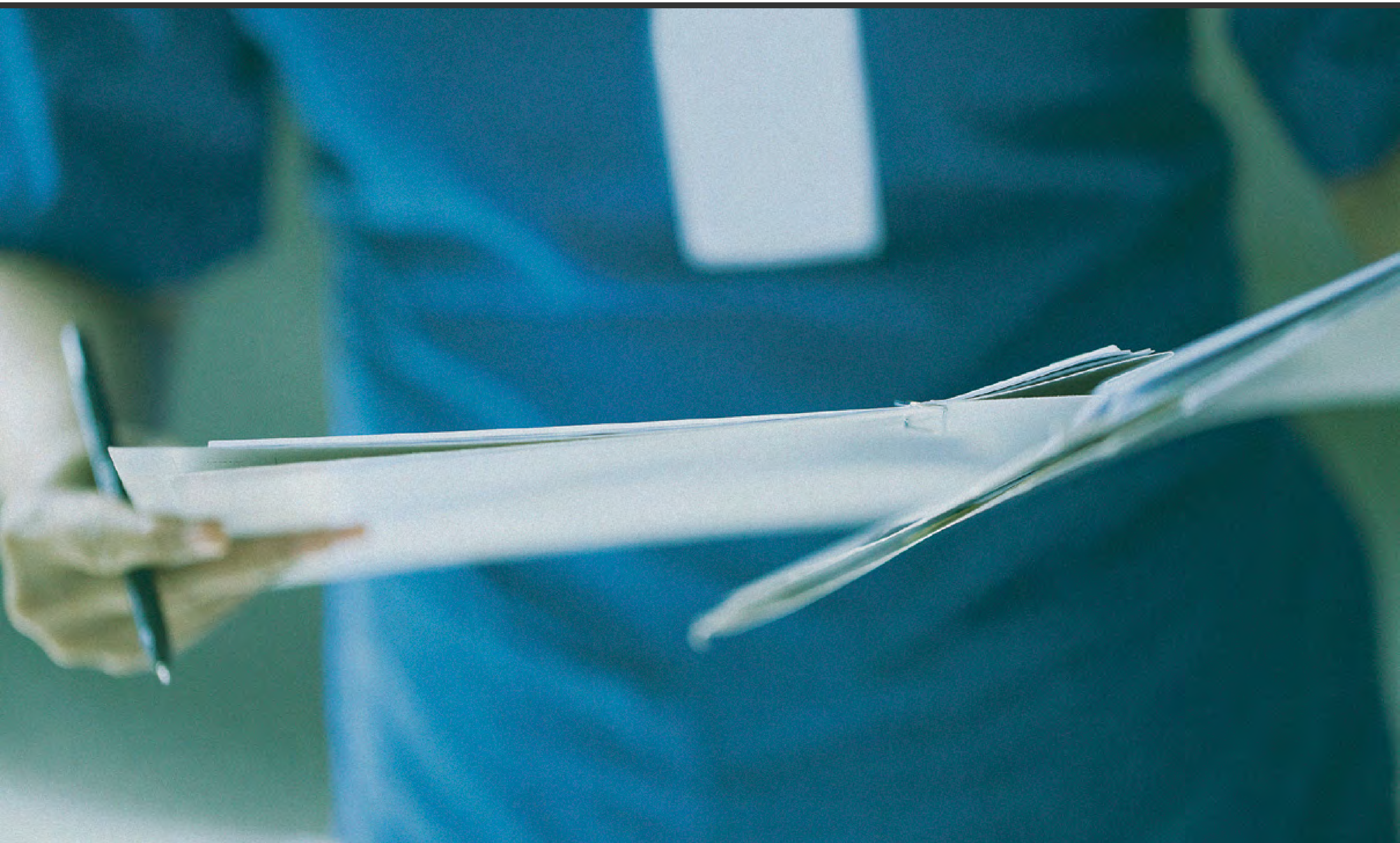
ARMOR™
BETWEEN YOU AND THE THREAT

Uncheck yourself

BUILD A SECURITY-FIRST APPROACH TO AVOID ‘CHECKBOX COMPLIANCE’

KAREN SCARFONE | **PRINCIPAL CONSULTANT | SCARFONE CYBERSECURITY**



About Karen Scarfone

Karen Scarfone is the principal consultant for Scarfone Cybersecurity in Clifton, Va. She was formerly a senior computer scientist for the National Institute of Standards and Technology (NIST), where she oversaw the development of system and network security publications for federal civilian agencies and the public. She has co-authored more than 50 NIST Special Publications and Inter-agency Reports during the past 10 years, including NIST Special Publications 800-111, Guide to Storage Encryption Technologies for End User Devices, and 800-123, Guide to General Server Security.

Scarfone Cybersecurity | NIST

Executive summary

An organization's information technology (IT) resources are subject to numerous regulatory compliance mandates to prove that they are protecting the sensitive data they store

Some of the most common include the Health Insurance Portability and Accountability Act of 1996 (HIPAA); the follow-on Health Information Technology for Economic and Clinical Health (HITECH) Act from 2009 and Omnibus Final Rule of 2013 for healthcare data; the Payment Card Industry Data Security Standard (PCI DSS) for credit and debit card data; the Federal Financial Institutions Examination Council (FFIEC) handbooks; and the Gramm-Leach- Bliley Act (GLBA) for financial data.

Because of the perceived importance of compliance, many organizations make the mistake of putting compliance first and security second. It is assumed — incorrectly — that achieving compliance necessarily implies sufficient security.

In fact, compliance is simply a reporting exercise whereby an organization documents or demonstrates how its security program addresses a particular set of compliance requirements.

"Because of the perceived importance of compliance, many organizations make the mistake of putting compliance first and security second."

As recent breaches (e.g., Target, Sony, Community Health Systems) have demonstrated, an organization can be compliant with PCI DSS, HIPAA or other industry or government regulations, yet still operate insufficient security programs that unnecessarily expose the organization to compromise from the constant stream of cyber attacks.

The intention behind compliance requirements is to serve as a minimum security bar for protecting the information that is subject to the requirement. As such, these compliance requirements should be seen as a baseline for an organization's security program.

That program should be driven by the organization conducting internal risk management processes to determine which security controls are necessary to protect the sensitive data they hold.

Organizations should focus their energy on implementing sound security programs based on identified risks. Once implemented, they'll find that this addresses all — or nearly all — of their compliance requirements.

"The intention behind compliance requirements is to serve as a minimum security bar for protecting the information that is subject to the requirement."

Conquer the compliance challenge

Compliance. The mere mention of the word conjures anxiety into the hearts and minds of many IT professionals. But compliance efforts were never meant to be so intimidating. Rather, they were designed to help ensure that all relevant organizations acknowledge a common set of basic information security concepts and controls.

Unfortunately, due to the way in which most requirements are written, and the wide variation in how they are monitored and enforced, achieving compliance is often more difficult in practice. This is compounded when organizations are subjected to multiple sets of requirements. When this occurs, it's no wonder many compliance officers feel like conceding out of frustration.

Each compliance effort uses its own terminology, organizes its requirements differently, and references disparate sets of security requirements and applies them to different degrees. For instance, the PCI DSS has 12 main categories of requirements, and it provides very prescriptive guidance.

HIPAA History

HIPAA is a U.S. federal law created, in part, to safeguard the security and privacy of certain health-related information, such as patient records.

Although HIPAA was passed in 1996, the accompanying Security Rule and Privacy Rule documents, which provide more details on the security and privacy requirements, were not finalized until 2003 and 2012, respectively.

HIPAA compliance has been required for a wide variety of organizations since shortly after the requirements were finalized.

HIPAA COMPLIANCE

In contrast, HIPAA consists of three main rules, each with their own organization. HIPAA is not very prescriptive and categorizes each control as either addressable (optional) or mandatory. It is, therefore, difficult to map or align them to each other. These requirements also evolve over time, some on a regular schedule (e.g., PCI DSS), but most with relatively short notice.

Another complication is that many organizations, lacking a centralized compliance function, have assigned responsibility for each compliance requirement to different groups. Human resources typically is tasked with HIPAA oversight, IT is often handed PCI DSS, and finance/accounting typically manages mandates like SOX and GLBA.

This further complicates the crossmapping exercise and results in overlapping efforts. In many cases, this means there are overlapping or redundant tools and processes, too. The result is that organizations are expending too many resources to ensure they meet every requirement in each compliance effort.

HIPAA Penalties

A range of consequences can occur to organizations based on violations of the HIPAA requirements. Any type of violation — be it an accident or the result of "willful neglect" — can result in a maximum fine of $50,000 per violation, capped at $1.5 million a year.

Individuals who violate HIPAA requirements can also be fined, up to $250,000 for the most serious violations, and prison sentences of up to 10 years are also a possibility.

Ignore compliance, focus on security

Given the difficulties in trying to solve the compliance problem directly, there must be an easier and more methodical manner to achieve compliance.

There is. And it begins with initially ignoring compliance requirements.

Wait. Ignoring them? How can you both meet and demonstrate compliance by ignoring them?

The answer: build a strong security program that addresses the risks your organization faces regarding the sensitive data you store and manage. As the basis for controls, this approach should use an industry-standard framework that will mitigate risks to an acceptable level.

Compliance is not a thing into itself, but rather the exercise of documenting and demonstrating how security controls meet a specified set of requirements.

Naturally, if you build a strong security program that addresses the risks to your organization's sensitive data, you will likely have solved most of your compliance requirements.

PCI DSS History

PCI DSS is a document that defines security requirements for businesses, educational institutions, government agencies and other organizations that handle credit or debit card data to ensure that data is safeguarded.

PCI DSS COMPLIANT

This approach will not always result in 100 percent coverage. But by addressing 80 to 90 percent of requirements, it is a relatively simple process to identify the remaining requirements that need to be solved. From there, you'll be able to add new controls, or modify existing ones, to correct any gaps.

Many compliance requirements are inherently risk-based. This requires you to conduct a risk assessment to identify the risks and determine which security controls will mitigate those risks.

There is significant overlap among the compliance requirements, so the risks for each type of regulated data your organization handles will be mostly the same. And all can likely be addressed by a consolidated set of controls.

So, how do you get started? Begin with the following five key risk assessment methodologies.

PCI DSS Penalties

There are serious consequences for organizations that fail to fully comply with the PCI DSS requirements.

Hefty fines can be levied against organizations for violations, and the most serious violations can result in a suspension of privileges for processing cards (although this outcome has not yet been realized).

PCI DSS COMPLIANT

The 5 risk assessment methodologies

Many organizations believe that risk management is a big, ugly beast and tend to stay away from it. Instead, they opt to find and follow checklists of typical security controls or ask their IT and security teams to recommend a set of tools without performing any analysis of the situation.

Unfortunately, taking either of these approaches generally leads to unsatisfactory results. Just look at the constant stream of data breaches that are reported in the news. Most people assume that large organizations have solid security programs in place. This simply isn’t the case.

So, how do you get started on a risk assessment? Begin by looking at the fundamental concepts behind security. A good source can be found in the opening section of the HIPAA law.

Using this as a guide, the goal of a risk assessment is to identify potential vulnerabilities and threats that exist in ensuring the confidentiality, integrity and availability of sensitive data you handle, and to protect it from reasonably anticipated security threats.

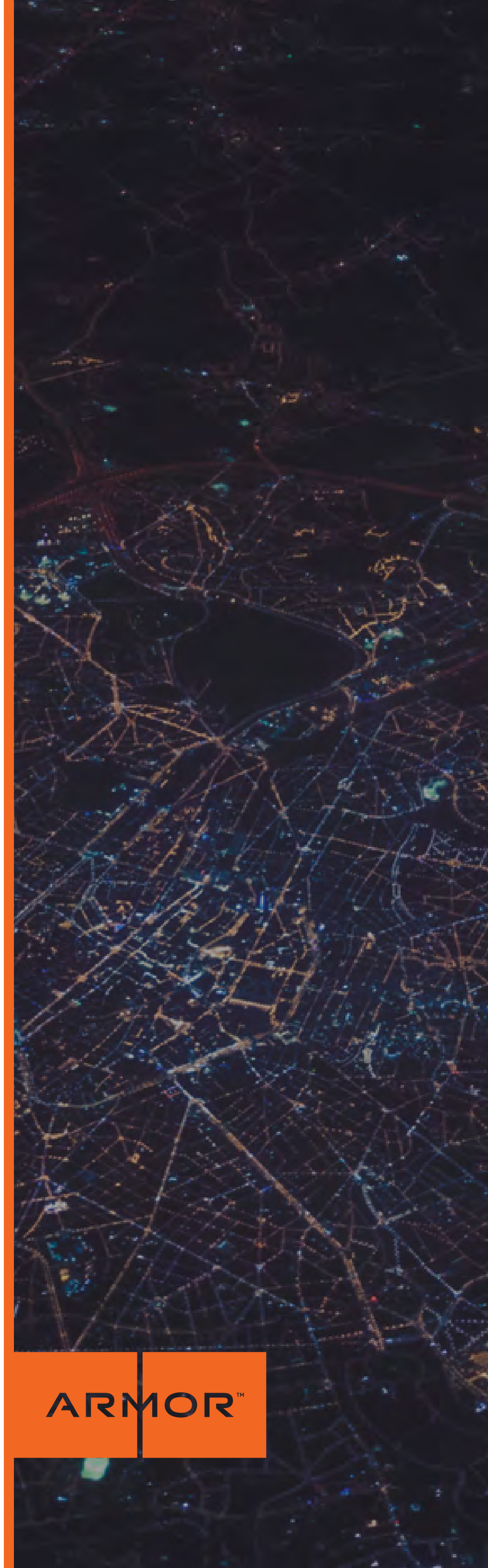
In simpler terms, organizations should develop a contingency plan for all possible scenarios within an environment that might cause sensitive data to be compromised.

There are several risk assessment methodologies that provide more specific steps and processes for conducting a risk assessment (see “Risk Resources” on page 11).

§ 164.306 HIPAA Security Standards: General Rules

General Requirements. Covered entities must do the following:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity creates, receives, maintains, or transmits.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.



Build your security controls program

Once you have the results from your risk assessment, use them to either build a new security program or evaluate your current strategy.

In either case, you need to document the controls that have been selected, along with the details of how they will be implemented, monitored and measured.

This is no small task. But if done correctly, with the right amount of detail, it will help demonstrate how your program meets the organization's compliance requirements. It's important also to consider that this security program may not meet 100 percent of your compliance requirements. And that's perfectly acceptable.

To complete your program, compare the list of controls you have developed to any specific requirements within the compliance regulations you need to address. This is not always easy, but in most cases the specific and detailed requirements are fairly easy to spot and highlight.

For instance, some have requirements around password length, complexity and rotation. These will be stated with specific numbers, so they are the easiest to identify. Others, such as authentication requirements — especially those requiring multiple factors — can be stated in terms like "strong authentication" or "that ensure the identity of the person."

The 5 risk assessment methodologies

1. **Identify potential risks**
   What could go wrong?

2. **Measure likelihood & impact**
   What is the likelihood of the risk occurring and, if so, what is the impact on the organization?

3. **Examine alternative solutions**
   What are the potential ways to treat the risk and, of these, which strikes the best balance between being affordable and effective?

4. **Decide which solution to use & implement**
   Find the needed resources, get the necessary buy-in and pull the trigger.

5. **Monitor results: Is your plan working?**
   Are changes or updates required?

> " ... this security program may not meet 100 percent of your compliance requirements. And that's perfectly acceptable."

ARMOR™

Task individuals, who are knowledgeable with the regulations, to review each and retrieve any specific or detailed requirements. This will help the group that is responsible for the security program compare the program with the requirements and ensure all are being met.

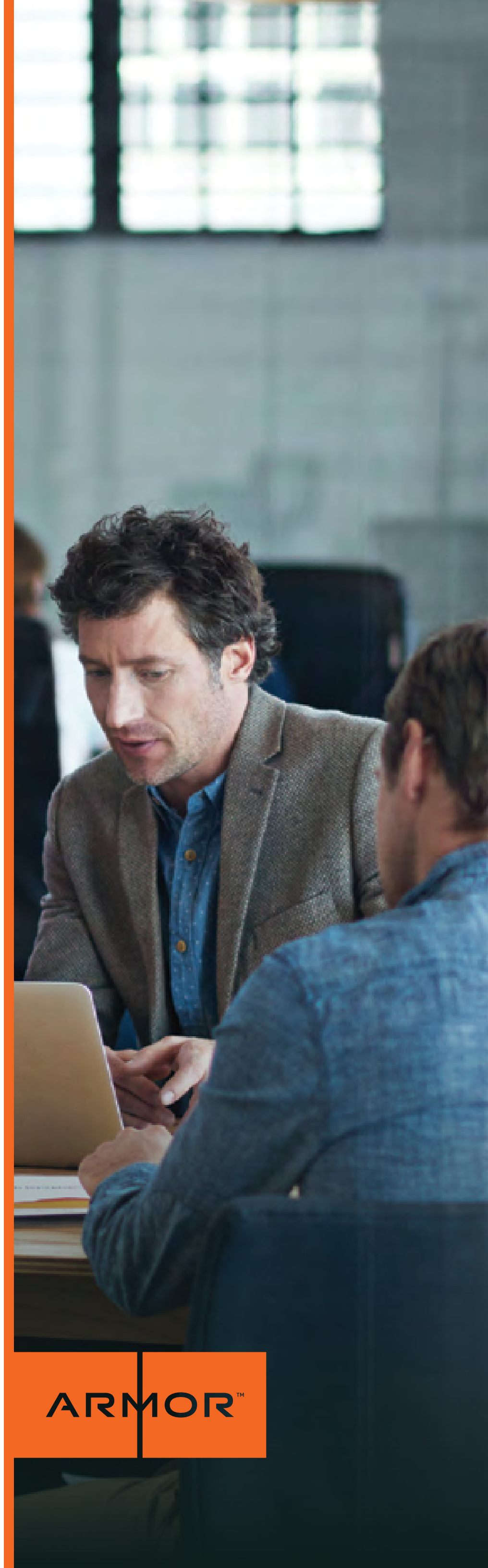
In some cases, this may mean adding controls to the program or modifying existing controls.

The end result of this exercise will be a strong, consolidated security program that you can be confident will meet your organization's specific compliance requirements. With this program in place, demonstrating compliance with any of the requirements becomes a reporting exercise. You'll match deployed controls against requirements and prepare a description of how you are addressing each.

If you are required to have a third party validate that you are meeting the requirements, the necessary information will be readily available. This approach makes the process quicker and easier on the organization.

PCI Compliance: By the numbers

12	396
Requirements	Distinct controls



Avoid 'checkbox' compliance

All too often, an organization's vision for achieving security simply involves checking the compliance boxes, without a deeper security strategy It is often tempting to take this approach, especially given some of the validation requirements.

Take PCI DSS validation, for instance. If your organization processes fewer than 1 million transactions a year, you can self-assess using one of the provided Self Assessment Questionnaires. These must be completed annually and sent to the organization's bank or processor. There is no oversight and they are seldom reviewed, so many organizations are very tempted to simply answer all of the questions "yes" and move on.

However, it only takes a brief glance at the headlines to know that achieving compliance does not equal achieving security.

Take the aforementioned Target breach as an example. Target was PCI DSS-compliant, yet weak authentication practices, failure to monitor controls and other security shortcomings allowed attackers to breach the company and steal nearly 70 million records. There's no better way to illustrate that compliance does not provide sufficient security.

To safeguard sensitive data against current threats, organizations must perform periodic risk assessments and use them to build and update a strong security program, then expend the necessary resources to implement, monitor and maintain those security controls.

This approach will not only provide a much stronger security posture, but it will also make it easier to achieve compliance requirements and ensure you are really protecting the data — instead of just checking the compliance box.

> "It only takes a brief glance at the headlines to know that achieving compliance does not equal achieving security."

Conclusion

PCI DSS, HIPAA and other compliance initiatives are meant to serve as a baseline of security controls that every organization should implement.

Most compliance initiatives are not overly prescriptive because they recognize that every environment and organization have unique characteristics that may make one solution more effective than another.

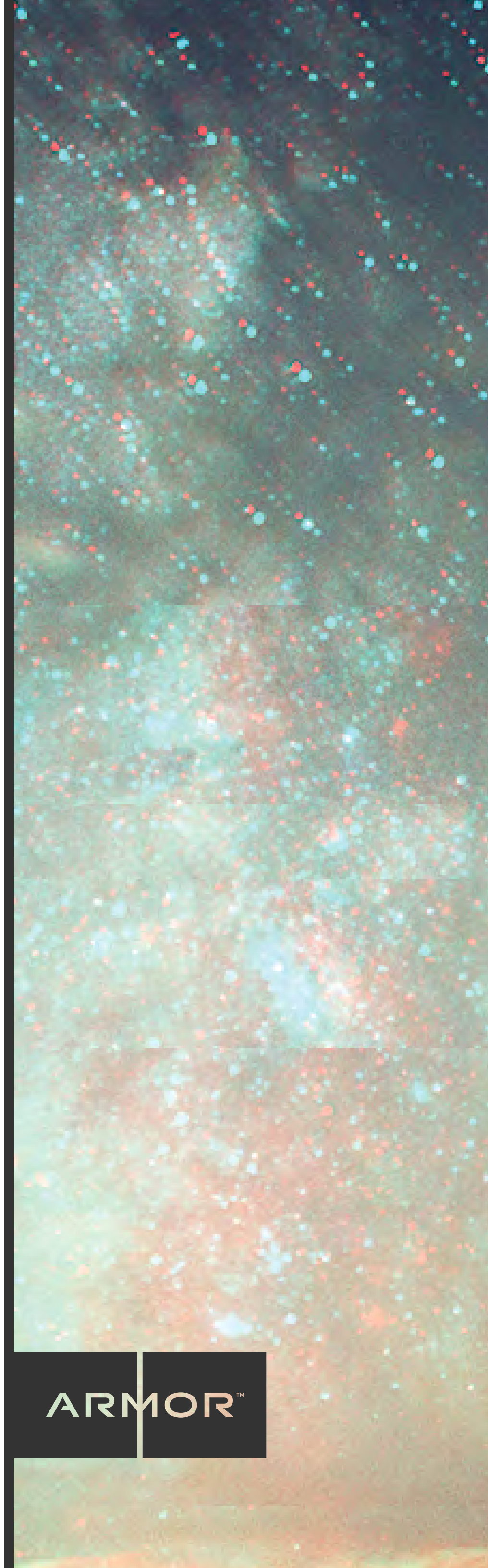
Rather than strictly directing organizations on exactly what they have to do to comply, the guidelines leave it up to organizations to analyze available security controls, as well as internal needs, in order to determine which security controls are required.

Unfortunately, many organizations are under the impression that achieving compliance also means achieving sufficient security. This is simply not the case.

Understand that compliance is simply a reporting function of a sound security posture. As the pervasive theme throughout this paper, organizations should focus on security, not compliance. By devoting adequate resources to countering today's threats, organizations will find that they meet all or nearly all compliance requirements, simply by following sound security practices.

Risk resources

- NIST guide for conducting risk assessments
- CERT octave
- RMI's FAIR basic risk assessment guide
- ISO 27005: Information security risk management
- ISACA risk IT framework



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