FISMA COMPLIANCE:

PRACTICAL STRATEGIES

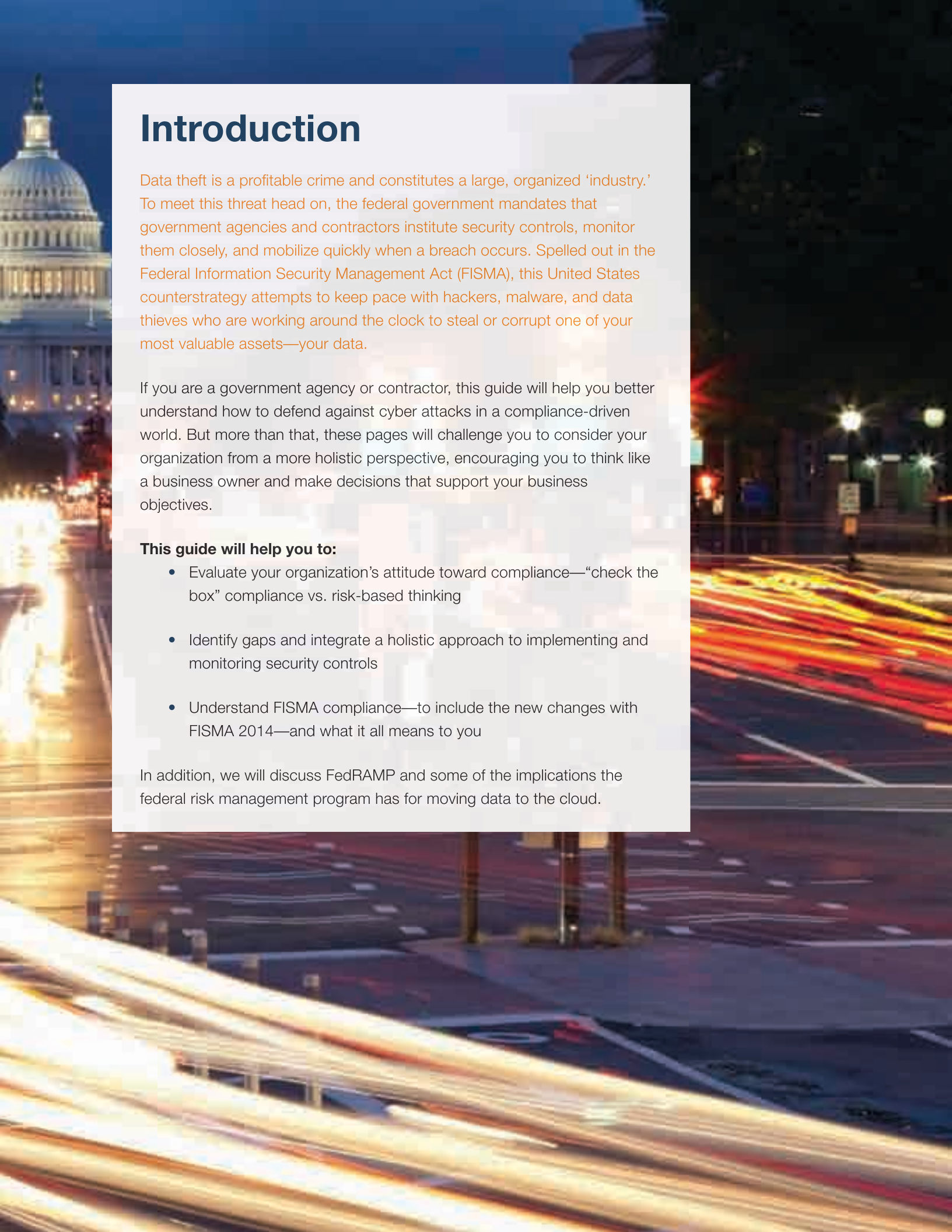
LBMC Security & Risk Services

FISMA Compliance: Practical Strategies

Published by LBMC Security & Risk Services, LLC
Nashville, Knoxville, Chattanooga

Design by Hinge. Visit our website at www.hingemarketing.com

Table of Contents



Introduction

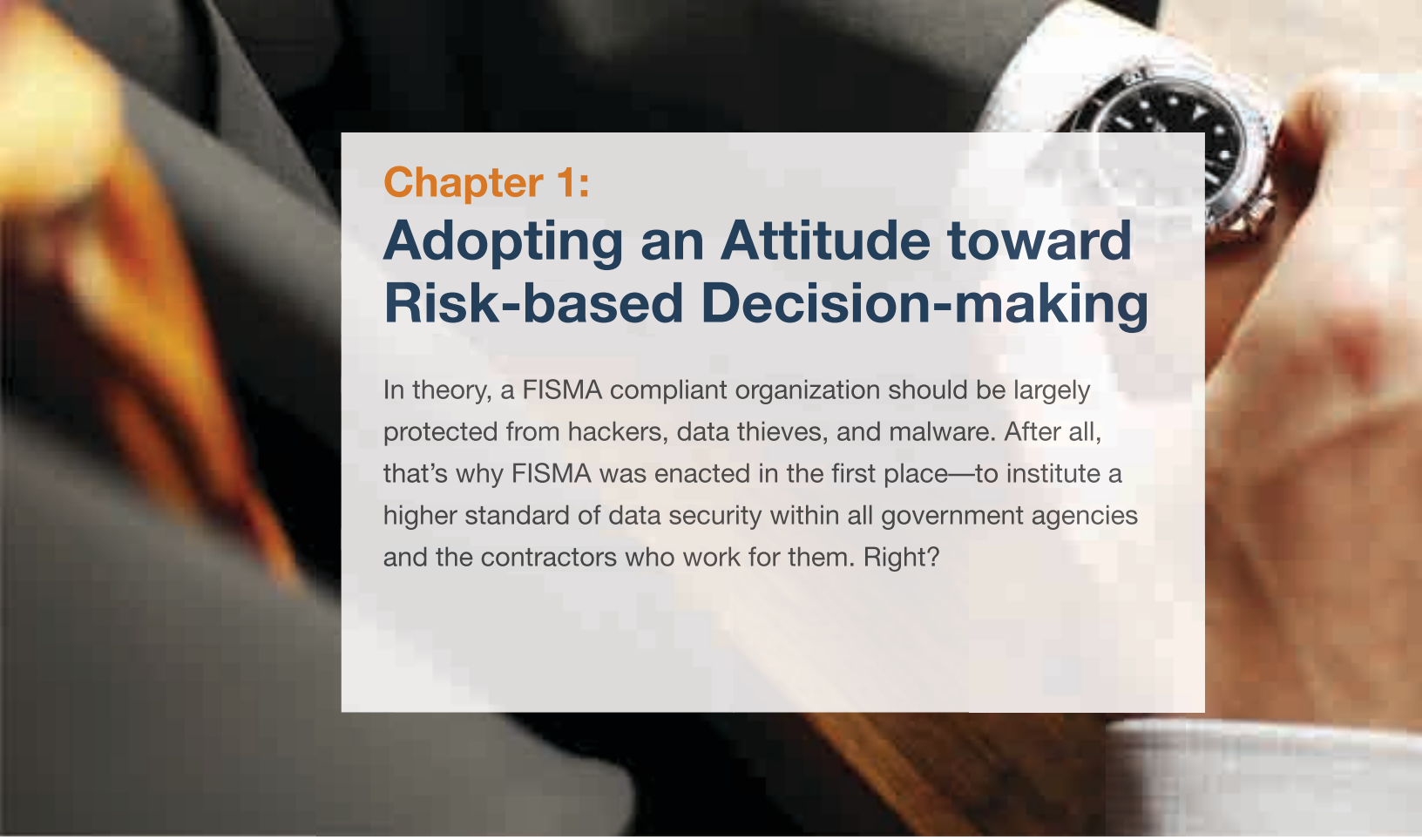
Data theft is a profitable crime and constitutes a large, organized 'industry.' To meet this threat head on, the federal government mandates that government agencies and contractors institute security controls, monitor them closely, and mobilize quickly when a breach occurs. Spelled out in the Federal Information Security Management Act (FISMA), this United States counterstrategy attempts to keep pace with hackers, malware, and data thieves who are working around the clock to steal or corrupt one of your most valuable assets—your data.

If you are a government agency or contractor, this guide will help you better understand how to defend against cyber attacks in a compliance-driven world. But more than that, these pages will challenge you to consider your organization from a more holistic perspective, encouraging you to think like a business owner and make decisions that support your business objectives.

This guide will help you to:

- Evaluate your organization's attitude toward compliance—"check the box" compliance vs. risk-based thinking
- Identify gaps and integrate a holistic approach to implementing and monitoring security controls
- Understand FISMA compliance—to include the new changes with FISMA 2014—and what it all means to you

In addition, we will discuss FedRAMP and some of the implications the federal risk management program has for moving data to the cloud.



Chapter 1:
Adopting an Attitude toward Risk-based Decision-making

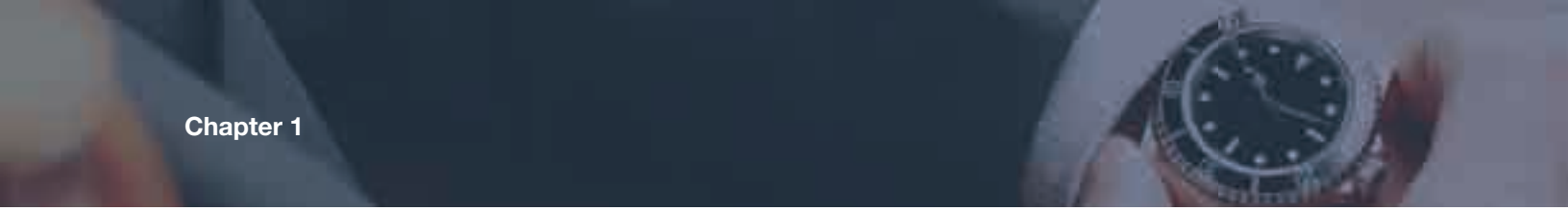
In theory, a FISMA compliant organization should be largely protected from hackers, data thieves, and malware. After all, that's why FISMA was enacted in the first place—to institute a higher standard of data security within all government agencies and the contractors who work for them. Right?

Think again. As with many noble government initiatives, the real-world translation of FISMA might not be having the far-reaching impact that was hoped for. One of the biggest complaints about this regulatory act is that FISMA takes a boilerplate approach, mandating minimum security measures and burdensome reporting, rather than addressing *actual* threats to the well-being of the organization as a whole.

If you are an entity doing business with the Federal Government or you are the Federal Government, compliance with FISMA regulations is mandatory. The good news is, many of the mandated safeguards will keep your data safer. But a smart organization will adopt a broader perspective on protecting data by taking a risk-based approach and figuring out what's at stake behind each decision.

Compliance vs. Risk-based Decision-making

Your data is one of your most valuable assets. Just as you would when introducing a new product, investing in capital equipment or taking on a new business partner, you will want to make your decisions about security controls based on the amount of risk you can tolerate. Here are some of



the questions you might want to ask: How proprietary and sensitive is the nature of your data? What kind of impact would it have on your business or operations if someone stole or gained unauthorized access to this data? Do you have the resources needed to contain a serious breach? A vicious spear phishing attack?

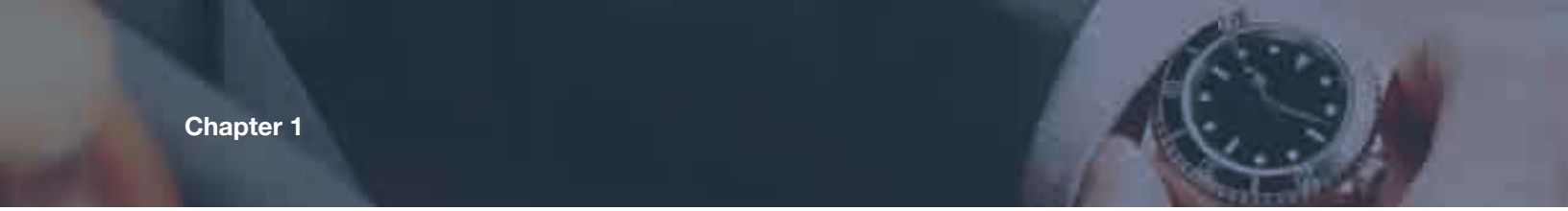
Organizations that take a risk-based approach tend to think through each major decision with regards to security controls and conduct a risk assessment or a cost/benefit analysis to decide whether or not to move forward. Rather than being reactive when incidents occur (or an audit is coming up), this type of organization develops a thoughtful data security plan to assess security gaps, implement appropriate controls, monitor and validate compliance, and mobilize should a breach occur. The key takeaway here is that the entire program revolves around the impact an incident would have on the organization as a whole—and on each of its individual business units.

Oftentimes, a risk-based security solution goes beyond compliance. Take your system passwords, for example, which may be required to have an eight-character length. Should you adopt an eight-character password in order to be compliant? Possibly. However, if upon examination you conclude that you need better control over access to your system, you might consider instituting a ten-character password instead.

But don't stop there. Generally speaking, passwords are not a particularly airtight form of authentication. Consider a stronger multifactor ID, like a token, biometric or callback authentication. Even if the compliance requirement doesn't mandate this, you can if the business risk warrants this control.

In other words, meeting compliance *might* be all you need to do. But don't just accept it as such. Analyze each requirement and its implications for your business before making a decision.

Granted, it's not always clear what to do. One organization we know of had fallen below compliance in a particular area, thereby incurring fines of $20,000 per month. The executive team decided they were willing to pay the fines and accept the level of risk the infraction posed, rather than invest the 6-8 million dollars required to fix the problem. They chose this route largely because they had other revenue-generating initiatives competing for



those same dollars. Maybe if the team had factored the business risk and associated costs of a major breach into their decision-making process, they would have decided differently. Aside from the direct costs of recovering from a breach, the loss of goodwill and public trust need to be factored in as well. However, we applaud this executive team for weighing their organization's business needs against the commensurate risk before making a decision.

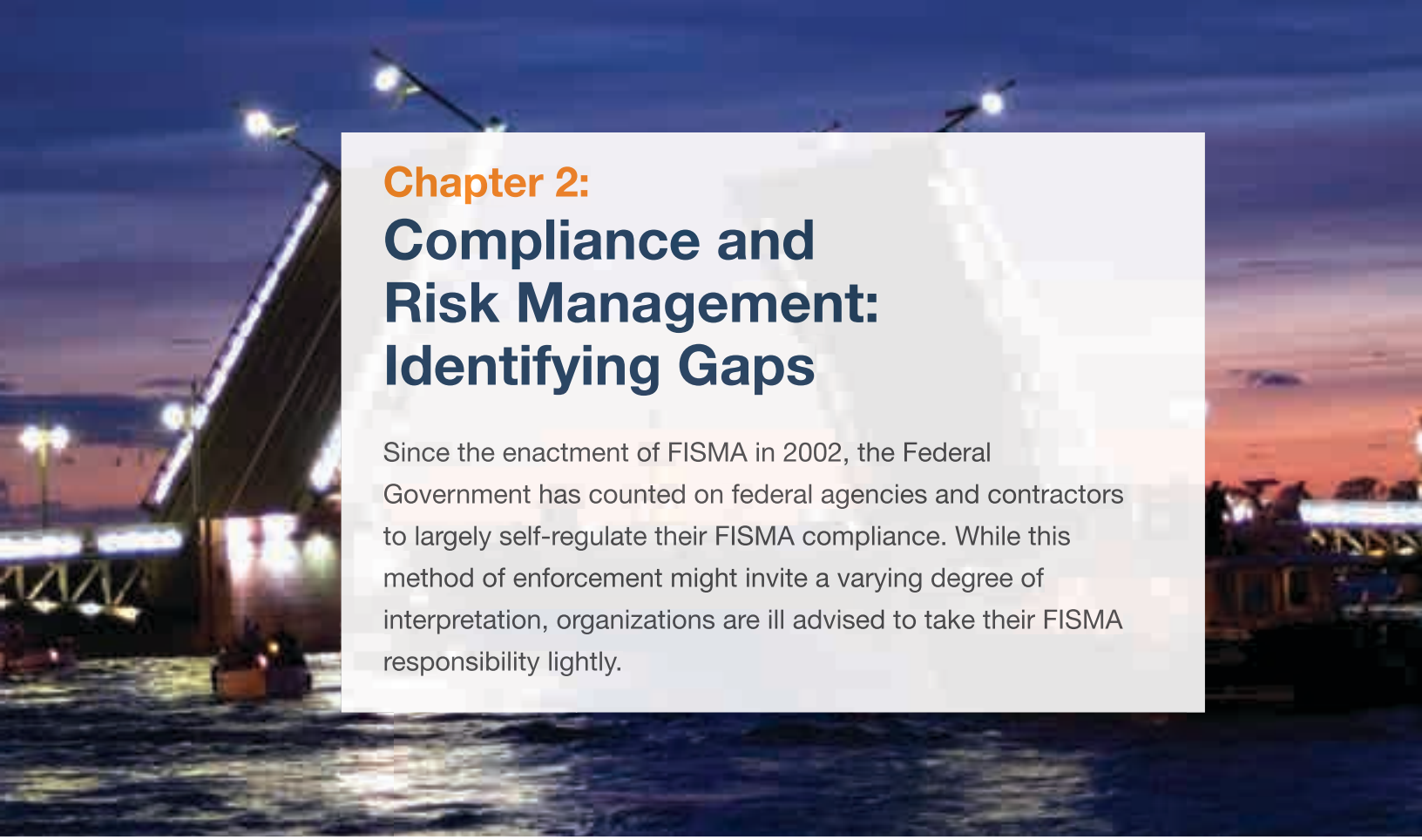
Benefits of Risk-based Decisions: Going Beyond Data Security

Organizations that adopt a risk-based approach place a premium on protecting their data as it pertains to the viability of their business. As such, they tend to have tighter but practical security controls in place, which confers upon them added rewards.

Competing for government contracts is one area where taking a risk-based approach may benefit you. A pro-active, risk-based data protection strategy can be a differentiator that puts you in a better competitive position, as many companies are struggling to even meet compliance. We saw companies take a risk-based approach to data security years ago when FISMA was just getting off the ground, and those companies have consistently won new contracts as a result of their ability to verify that their systems are safe.

In short, choosing a risk-based approach aligns data security with business strategies. Communicating to the board and executive management about proposed security controls becomes more relevant to them, as the implications tie in to areas of the business they deal with every day. Funding for controls is more likely to be granted when the powers-that-be understand the business reasons behind each request. The organization's security posture increases as responsibilities are pushed throughout the organization instead of relegated to an isolated policing function in the IT department.

By adopting such a forward-thinking stance, you will be doing the right thing by your organization. Furthermore, you will build an industry-wide reputation as a reliable partner to do business with.



Chapter 2:

Compliance and Risk Management: Identifying Gaps

Since the enactment of FISMA in 2002, the Federal Government has counted on federal agencies and contractors to largely self-regulate their FISMA compliance. While this method of enforcement might invite a varying degree of interpretation, organizations are ill advised to take their FISMA responsibility lightly.

The Office of Management and Budget (OMB) has been authorized to enforce compliance, and it's within their power to penalize you if you don't comply. And as of the 2014 updates, the Department of Homeland Security (DHS) will have its eye on you, too.

As an agency, if you incur a serious infraction, Congress may opt to reduce your information systems budget. You could also be restricted as to which private contractors you are allowed to use, and if you *are* a contractor, your award fee may be negatively impacted by repeated non-compliance. And be aware that an agency's failing grade can also be made public.

FISMA violations are serious, which is why it's important to get a handle on one of the most important steps to compliance—the FISMA Assessment.

FISMA Assessments: The Fundamentals

Inherent in FISMA are strict (and oftentimes onerous) requirements. To satisfy this mandate, agencies and contractors conduct regular assessments to determine how they are performing as prescribed by the NIST 800-53 control requirements. Some organizations conduct this audit

internally using an internal audit function, while others outsource it to a third party. With either approach, the executive management team is ultimately responsible for reporting on identified risks and evaluating the effectiveness of an organization's security controls.

So what are the main components of a FISMA assessment? As with most audits, you will want to include each of the following:

- Interview the individuals responsible for the control documentation process to gain an understanding of the overall process and key contacts and control owners.
- Gain an understanding of the current processing environment to determine where commonalities are expected within the control environment.
- Determine an appropriate sample size and characteristics for each of the control areas under review.
- Conduct a performance review audit using the NIST Assessment Methods and Objects to achieve the Assessment Objectives.
- Document testing results within the FISMA Assessment Report.

As you can imagine, a FISMA Assessment can be fairly disruptive and is often greeted with a general air of trepidation. Collecting supporting documents takes time away from daily operations, and most people are hesitant to build a case against themselves by helping auditors find issues. Process owners may become defensive or even try to conceal areas of control weakness.

That said, there *are* ways to lessen the inconvenience and threatening nature of an audit. Gather the key players and enroll them in your vision: an assessment is an opportunity to protect the company's assets and reduce the number of security incidents. Help your staff understand how the assessment will facilitate change for the better, and be sure to provide a list of supporting documentation that each stakeholder is required to submit so your staff can be prepared in advance.

You want to challenge your staff to ‘better their best.’ If they understand the value of the assessment, they will be more likely to cooperate and work toward the common goal of having a better-protected system.

As a best practice, the audit team should make an effort to give credit where credit is due, which audit teams oftentimes fail to do. While lapses in a policy or procedure update shouldn’t be sugarcoated, it’s important to balance the findings by identifying what’s working. If you are seeking an outside vendor to conduct your assessment, make sure they are prepared to partner with you and your staff, rather than creating an environment of fear and generating findings to justify their fees.

You want to challenge your staff to ‘better their best.’ If they understand the value of the assessment, they will be more likely to cooperate and work toward the common goal of having a better-protected system.

Building a Solid Foundation

Many organizations struggle to even cover the basics. They are constantly putting out fires and struggling to respond to new threats. They tend to perform poorly in audits. In fact, this type of organization is often unable to get out of audit mode, continually finding themselves responding to findings or scrambling to prepare for the next audit.

To counter this and to build a secure environment down to its core, we recommend implementing a solid foundation of security controls in several key areas. This set of controls will serve as a strong base and will eliminate the root causes of most high-risk audit findings. The initial effort to do this is costly, but in the long run, you will save time, money, and headaches; and your data will be more secure.

We recommend that you evaluate the following process areas and institute a foundation of strong controls in each:

Information Technology Asset Tracking: Maintaining a controlled and accurate inventory of all IT assets is a critical underpinning of any information security program. The basic premise here is that you can't control what you don't know you have. For example, if an employee checks out a loaner laptop and doesn't connect to the network for an extended period of time to update system patches, that system is officially in an insecure state. The unaccounted-for laptop has potential to show up at the worst possible moment—during an audit, of course, or when a malware outbreak is scanning your system for vulnerable machines.

Evaluate your current IT asset inventory process and develop an enterprise approach to managing these assets across all business units and facilities. By carefully examining your business units, the flow of IT assets within your facilities, and the interrelationships of the departments that need IT asset tracking, system requirements can be defined to drive solid processes and an appropriate tracking solution.

Configuration & Patch Management: In today's threat environment, strong configuration and patch management are vital to ensure that systems do not fall victim to malicious software and attacks. Historically, many would consider a 95% patch rate as very good, but today we have to be nearly perfect to be effective. The bar has been raised dramatically due to automated hacker tools that scan networks, looking for vulnerable systems. Configuration standards need to be developed for all major applications and general support systems. Furthermore, these configuration standards must be consistently implemented and continuously monitored for compliance at all times.

Change Management: Effective change management is one of the most important core elements of a sound control environment. Establish an upper management control board to review changes and make risk determinations. Ideally, board members will serve for a long time, as continuity of this group is critical to ensure consistency of treatment for each type of request or change. The board is responsible for evaluating and accepting the risk of each change based on the following factors: the inherent level of risk in the change, the adequacy of test plans and related results, and possible backout procedures in the event of an issue.

Access Controls: User access control is a multi-faceted area that encompasses user identity management, facility access, and authorization from cradle-to-grave—from on-boarding a new user, through transfers, promotions, and termination. It is critical that procedures are put in place to notify the IT department immediately when there has been a change in an employee's status. Password configurations, levels of access, equipment assignments, remote transaction permissions, and facility accessibility all need to be considered and changed on a regular basis.

System Event Monitoring: Done manually, this control requires a massive amount of human capital to perform effectively. Even then, the ability to do the job manually is questionable. Automating this process is far superior in today's threat environment; it is advisable to deploy centralized logging and monitoring solutions to ensure that all major applications and general support systems are being monitored around the clock. Systems must be tuned and rules developed, which is an ongoing process as the threat environment is constantly changing. Consider using advanced techniques such as "honey tokens" to find anomalies. Having a robust anomaly detection strategy is the best defense against APTs, spear phishing, and zero day attacks.

Documentation Requirements & Formality: Documentation must be accessible to those who use it, updated as changes occur, and at your fingertips during an audit. A centralized repository of documentation is recommended; use of a single product on a corporate-wide basis is typically the best solution. That said, for many companies, the migration from a disparate system to a centralized one is a significant undertaking.

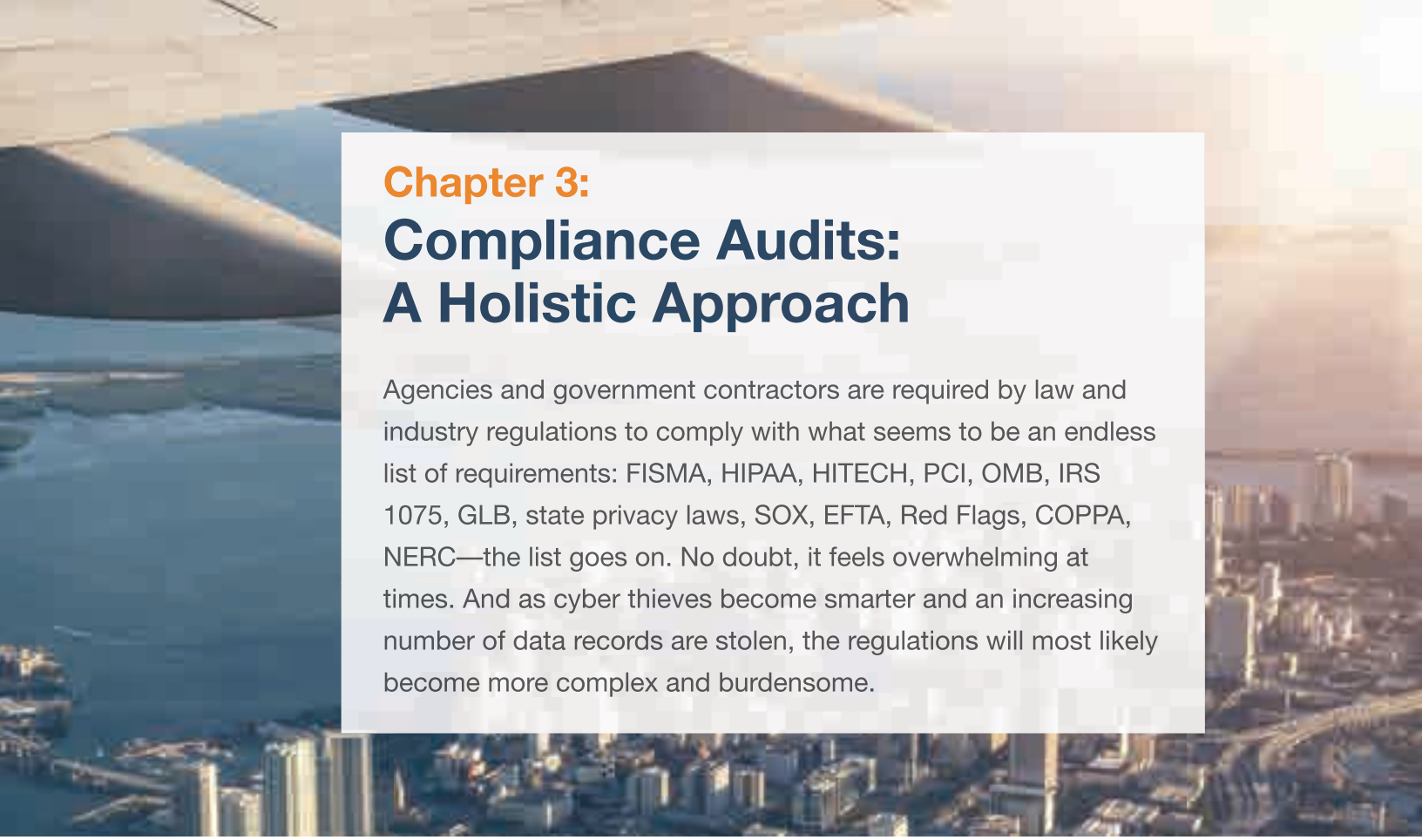
We suggest the following approach:

- Inventory all existing policies and procedures; corporate-wide is recommended, but IT-wide is a minimum
- Identify gaps between required and existing documentation
- Document the desired business process to maintain documentation
- Determine the user population for the document repository and level of access needed

- Document the requirements and desired features for a robust solution
- Determine if a new solution is needed or if use of an existing solution can be expanded
- Define document templates—enforcing an organization structure and use of templates is critical to a successful implementation

Testing & Validation: A common characteristic of high-performing security programs is an integrated testing and validation program. On an on-going basis, validate current processes in light of both compliance requirements and the threat environment. The key to a successful testing & validation program is the ability to subsequently hold stakeholders responsible for controls and make improvements as appropriate. A testing and validation program should not be viewed as a policing activity; rather, it should have a philosophy of continuous process improvement and innovation. Testing and validation will necessarily include: annual FISMA assessments, penetration testing, security testing, and due diligence testing on new technology and connections.

By methodically working your way through each of these critical control areas, you will uncover gaps in your system and overlapping tasks that can be consolidated. This, in turn, will lay a solid foundation for taking a more holistic view. A solid foundation will minimize or eliminate high-risk audit findings, make external audits much more tolerable, and most importantly, help you manage risk at levels commensurate with your business needs.



Chapter 3:

Compliance Audits: A Holistic Approach

Agencies and government contractors are required by law and industry regulations to comply with what seems to be an endless list of requirements: FISMA, HIPAA, HITECH, PCI, OMB, IRS 1075, GLB, state privacy laws, SOX, EFTA, Red Flags, COPPA, NERC—the list goes on. No doubt, it feels overwhelming at times. And as cyber thieves become smarter and an increasing number of data records are stolen, the regulations will most likely become more complex and burdensome.

Not painting a pretty picture right? Well, there is a better way to tackle this alphabet soup of resource-consuming regulation.

We recommend taking the "thirty-thousand foot view" and considering your organization as a whole—identify commonalities across all of your reporting requirements and coordinate efforts, thereby reducing redundancy. Develop a crosswalk that aligns all of your organization's compliance requirements. This will allow you to identify the common enterprise controls that can be tested once and used many times to satisfy all reporting requirements. Then, on a case-by-case basis, you can tackle the outliers and 'one offs' that associate with a limited number of compliance requirements or specific lines of business.

This holistic approach will result in fewer hours spent responding to audit requests and should significantly reduce audit findings. A fragmented approach to compliance leads to "audit fatigue," and we all know that when we get tired we tend to get sloppy. Unfortunately, sloppy leads to audit findings and compliance gaps.

One of the biggest obstacles to a coordinated 'test once report many' strategy is time. And indeed, it takes a significant upfront effort to evaluate each compliance requirement and to coordinate the reporting effort. Additionally, it requires an individual (or team) that has a high degree of familiarity with multiple compliance requirements. But it's worth it. Not only will you save money in the long run by increasing the productivity of your staff and reducing the disruptive nature of audits, you might even find that you can reduce the direct expenses associated with compliance. Imagine your cost-savings if you could let your IT team focus more on innovation and development instead of spending so much time responding to audits.

Standardizing Your System and Processes

When an organization institutes a standardized system configuration and supporting processes, fewer resources are able to manage a larger number of security controls. For example, if the entire organization adopts a unified configuration for the Windows server(s), it's easier to disseminate security fixes and to monitor individual workstations for anomalies. Compliance also becomes significantly less taxing when you deploy a standardized array of hardware and software platforms.

But it's not just your platforms you'll want to consider. If each business area is implementing and monitoring controls and managing artifacts in its own way, FISMA compliance can be unduly burdensome. By standardizing your processes, you will reduce redundancies, increase the integrity of your reporting, and make it easier to fix what's broken. For example, let's say you've put a standardized change management policy in place that includes a ticketing system, request & approval process and implementation. Once you've determined that each component is solid, you can test single samples to find out whether or not the process is working across multiple environments.

By standardizing change and patch management, assigning a uniform handling of artifacts, codifying monitoring procedures, and adopting a centralized content management system for reporting, you will more easily be able to submit audit responses in a timely and thorough manner.

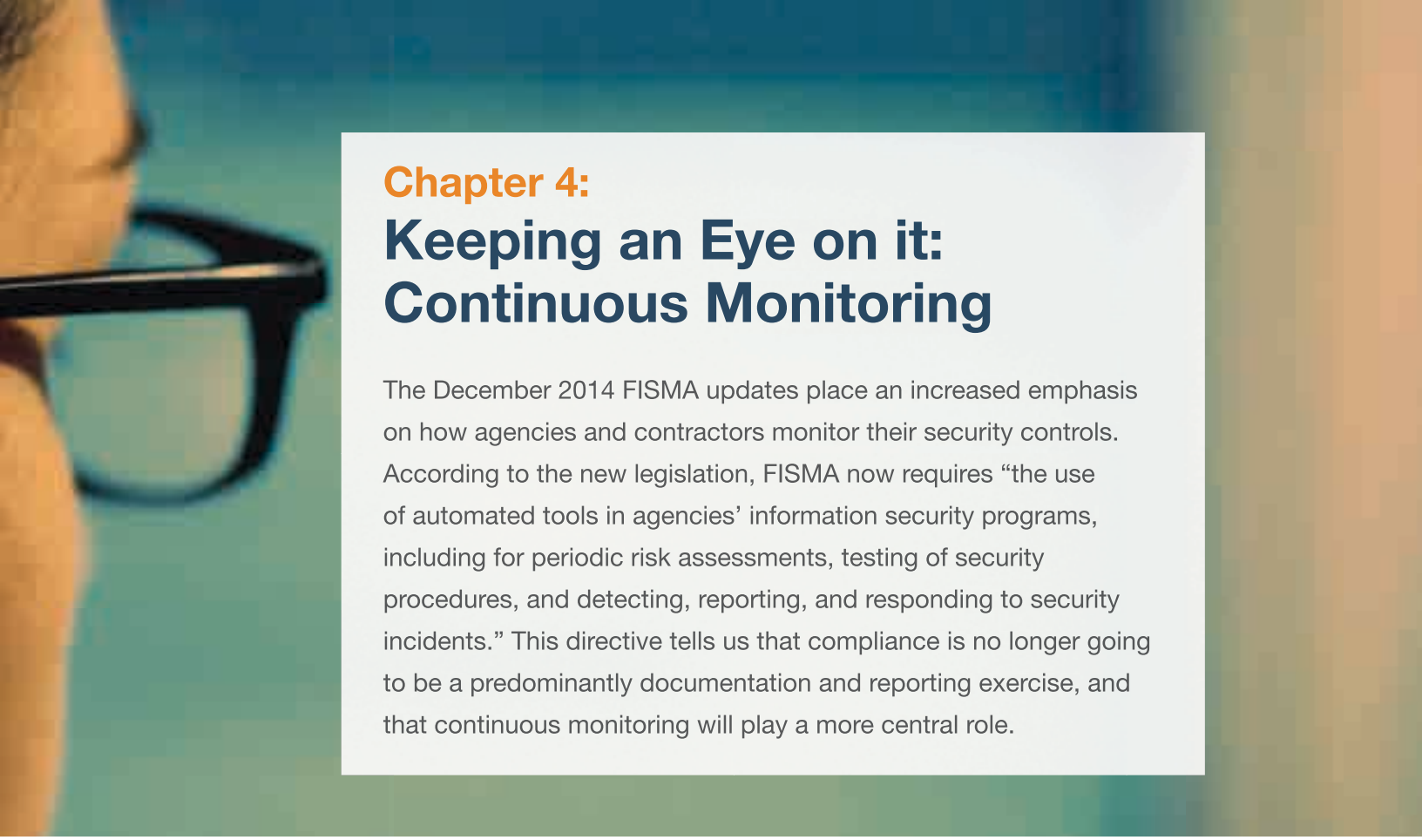
At first glance, the overhaul required to standardize technology platforms and processes might seem out of reach from a cost perspective. It's tempting to make do with what you have and adopt singular fixes that are

siloed around a compliance requirement or a particular security issue. But the cost of applying 'Band-Aids' adds up. Ultimately, your security solution becomes unwieldy, and your tools are no longer able to do what you need them to do. (Sometimes, they *never* did what you needed them to, and you were simply sold a bill of goods.) This ad hoc, reactive method of data security management may have lower direct costs, but the indirect costs of not having a standardized, organization-wide system can range from slow leaks to major hemorrhaging.

It's time to think differently about this. Total cost of ownership (TCO) is not typically reflected in the upfront pricing of what *looks* to be a cost-prohibitive solution. But do some research, and you might find otherwise. Toss around some 'what if' scenarios. Dig down into each application and business unit to determine what would happen if you *don't* invest in a data security strategy that encompasses a broader view. Find out how much more effective it is to make changes and monitor a standardized system. Check for redundancies that could be eliminated by a more holistic approach. You might quickly find that the TCO of standardizing your IT infrastructure and your procedures is much lower than what you are currently spending to put out fires.

By committing to a holistic approach, your entire data security compliance program will run more smoothly.

By committing to a holistic approach, your entire data security compliance program will run more smoothly. Should someone be out sick (or leave the company), another person can quickly fill in. IT platforms and tools are more uniformly updated and reconfigured. Process corrections can be made more easily. And you will definitely recognize economies of scale in the audit process. Not only will you be prepared for audit on shorter notice, more significantly, your controls will do a better job of keeping your data safe.



Chapter 4:

Keeping an Eye on it: Continuous Monitoring

The December 2014 FISMA updates place an increased emphasis on how agencies and contractors monitor their security controls. According to the new legislation, FISMA now requires "the use of automated tools in agencies' information security programs, including for periodic risk assessments, testing of security procedures, and detecting, reporting, and responding to security incidents." This directive tells us that compliance is no longer going to be a predominantly documentation and reporting exercise, and that continuous monitoring will play a more central role.

In other words, the government is moving away from a 'check-the-box' approach, which requires that agencies and contractors do so, too. The new FISMA legislation mandates that entities take a more proactive stance by appointing someone to mind the store at all times, and not just when an audit-reporting requirement is needed.

Continuous Monitoring: Going Beyond Data

Often times, audit findings and ongoing monitoring reports are organized in dashboards or report cards. While this type of reporting is useful, it's limited. Snapshot reporting is more granular around data and typically does not speak to the process. It *does* help identify performance gaps, but tends to elicit action around technical vulnerabilities and fixes, which might not solve the root problem.

It's critical to go beyond summary data and conduct ongoing validation and testing of your processes as well. Think creatively, here. For example, choose five random change management tickets and verify that proper procedure was followed. Were all of the stakeholders notified? Did the appropriate advisory board members have an opportunity to weigh in?

Was adequate testing performed? This type of sampling will help you identify procedures that are lapsing on a continual basis and/or individuals who are failing to perform the requisite tasks.

But don't stop there. It's important to not only check that procedures are being followed, but to also evaluate the process for its efficacy and alignment with business requirements. Sometimes, an organization will continue to perform a standard operation simply because 'they've always done it that way.' Under-performing processes become institutionalized, thereby weakening the effectiveness of security controls overall. Sure, validation tests help to verify that your staff is adhering to procedure, but regular testing also gives you the opportunity to challenge each initiative to make sure it's optimized and that it supports your business goals.

Adopting a Mature Model

In recent years, some agencies and contractors have begun migrating to a maturity model of cyber security implementation. These models are complex and take time to incorporate, but ultimately, the organizations that adopt them enjoy more sophisticated data security infrastructures. And while NIST standards are mandated guidelines for all agencies and contractors, many forward-thinking management teams are exploring other models to stimulate new perspectives and fresh thinking in their approach.

One example of a model highly regarded by multiple agencies is Carnegie Mellon University's Software Engineering Institute's Capability Maturity Model (CMM). As with all maturity models, rather than fighting constant fires, the CMM advocates creating a unified, enterprise-wide program that continues to improve as self-reported findings emerge.

According to this methodology, process maturity moves through five levels:

Level 1 - *Initial* Basic practices are in place, but performance is ad hoc. This may partly be a

reflection of the lack of experience on the team. It's difficult to move beyond this level without a concentrated effort to do so, since documenting weaknesses and learning from them are not a high priority here. Besides the drain on resources, this type of environment puts data at unnecessary risk and inhibits an entity from working toward its true mission and goals.

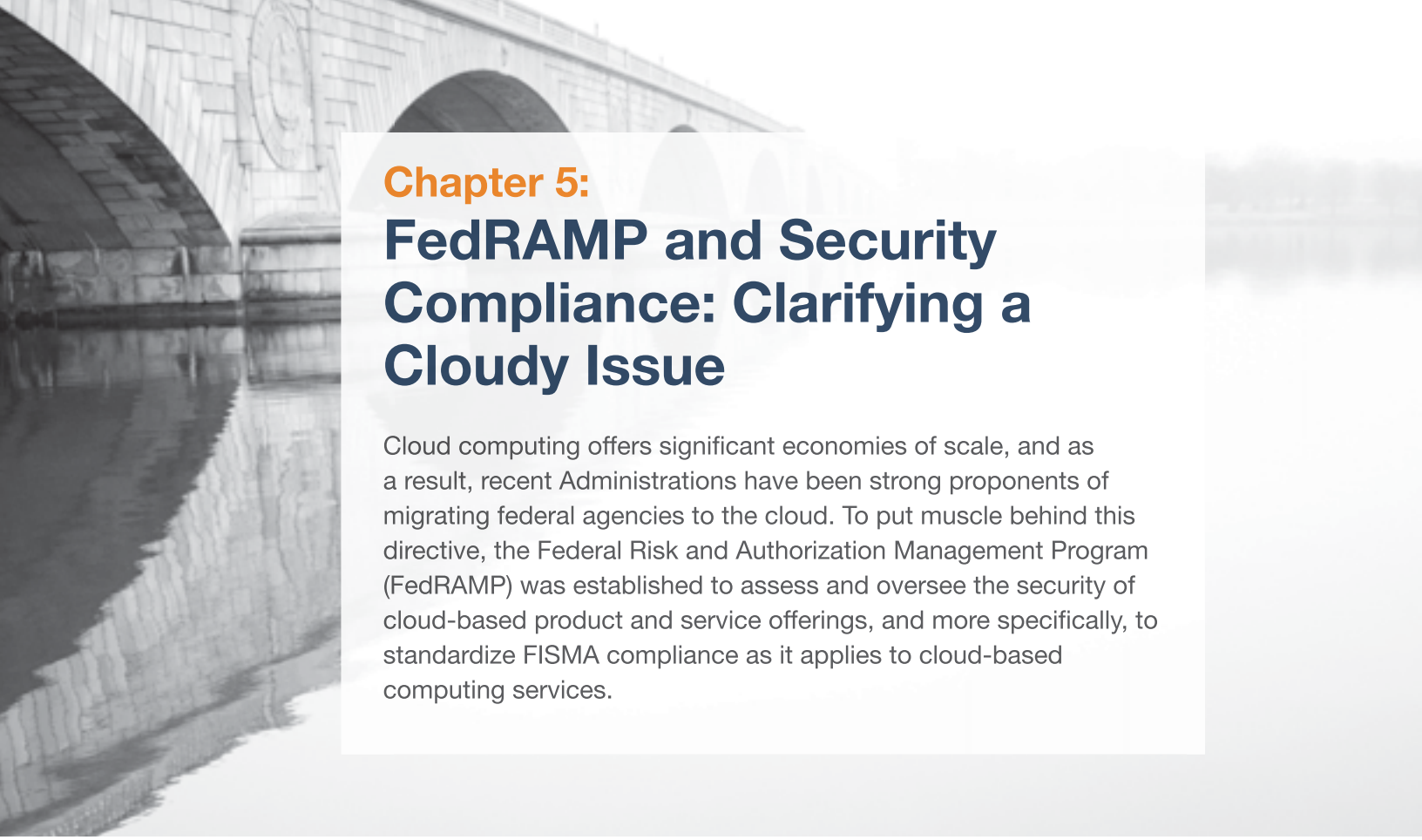
Level 2 – *Repeatable* At this level, management has put some processes in place that are carried out in a consistent way. While still a primitive structure, during a crisis, repeatable processes are more likely to be maintained.

Level 3 - *Defined* In level 3, there is a higher degree of standardization and more resources expended to support the process. The security controls environment is fairly stable throughout the organization and the stakeholders are better trained.

Level 4- *Managed* Here, process metrics are being implemented and management has more control. Processes are more readily adapted to particular projects while adhering to specifications and maintaining a high degree of efficacy.

Level 5 – *Optimizing* With a solid foundation in place, an organization at this level of maturation continues to identify areas of improvement. On an ongoing basis, they are constantly striving toward optimization across the enterprise.

As you 'graduate' to higher levels of maturation, policies and procedures become part of your institutional knowledge, independent of who is executing them. Over time, the CMM allows you to benchmark your outcomes with your findings, and against industry standards as well. Processes and procedures become more defined, documented, and repeatable. Security controls move toward optimization, and continuous monitoring becomes endemic to your process. You will also find that you have created a new organizational culture—one that places a top priority on securing data, and one that believes this noble goal can actually be accomplished.



Chapter 5:

FedRAMP and Security Compliance: Clarifying a Cloudy Issue

Cloud computing offers significant economies of scale, and as a result, recent Administrations have been strong proponents of migrating federal agencies to the cloud. To put muscle behind this directive, the Federal Risk and Authorization Management Program (FedRAMP) was established to assess and oversee the security of cloud-based product and service offerings, and more specifically, to standardize FISMA compliance as it applies to cloud-based computing services.

From a security perspective, the cloud is uncharted territory, oftentimes referred to as the 'digital wild west.' An increasing number of commercial enterprises are moving data to the cloud, and it follows that data 'bandits' are attracted to these well-stocked storehouses of information. For some agencies and contractors, relinquishing ownership of platforms, storage, applications, and connectivity to the cloud puts them in a quandary. Nervous about surrendering jurisdiction over compliance and security controls, these entities are struggling with the complexities of moving to the cloud and trusting that their regulated data will be safe.

But holding on to control does not necessarily equate with improved security. After all, most threat-vectors exist for on-premise data as do for the cloud, including mobile device monitoring, social engineering, and access control—to name a few. The recent flood of data breaches has not escaped the attention of the federal government, which is one reason FedRAMP was enacted in the first place. FedRAMP is a consorted effort by the government to adopt a 'do once, use many' approach to better secure *all* regulated data, and cloud computing might ultimately be the opportunity to make that happen.

Moving to the Cloud: Key Considerations

For starters, you'll need to partner with a Cloud Service Provider (CSP) who is FedRAMP certified. But just because a provider is certified doesn't mean you can stop thinking about FISMA compliance. Ultimately, your data's security rests on your shoulders, so specific details about security controls—and who is responsible for them—should be hashed out up front. How does your CSP perform audits? How do they monitor their data? How well do they segregate their FedRAMP-certified resources? What metrics are expected as part of your agreement with them? Make sure your contract spells everything out clearly, so you are not blindsided after you've signed up. Once on board, it can be extremely difficult to switch providers.

Separation from your data is another factor to consider. Controls will most likely be virtual rather than physical, and you may have no idea where your data resides. In fact, unless otherwise specified, some of your data could be 'living' in other countries. Cloud companies also share resources and services with each other, so it may not always be clear who is managing your data at any given time. All of these factors need to be considered up front.

Migrating to the cloud has its own challenges. It's important to ensure that your migration strategy is well thought out and reflects the needs of your business. Not every system, application, or service is a good fit for the cloud, so be sure to standardize (and document) your process for selecting the right candidates to migrate. If you are currently operating a legacy system, the transition is an opportunity to upgrade. But planning such a large-scale project—and its associated security risks—must be weighed when making this decision. Some entities opt to start small— moving email to the cloud, for example, but waiting until the concept is proven out before migrating more proprietary information such as personally identifiable information (PII) or electronic protected health information (ePHI).

Some of the key security issues to consider when working with a CSP are

1. Data encryption strategy (usually an add-on service offered by the CSP)
2. Access controls (both physical and logical)
3. Data backup, recovery, and destruction (exit strategy)
4. System integration issues (on-premise vs. cloud)

5. Intrusion detection/prevention, SEIM, and how the CSP implements and manages these technologies
6. Shared environment/platform issues
7. Ensuring high-risk data is saved in managed locations
8. How systems and data centers are monitored
9. Right to audit or assurance that controls are tested and validated

Again, these are issues you face whether you are using cloud or premise-based computing. Be aware that moving to the cloud does not allow you to abdicate these responsibilities.

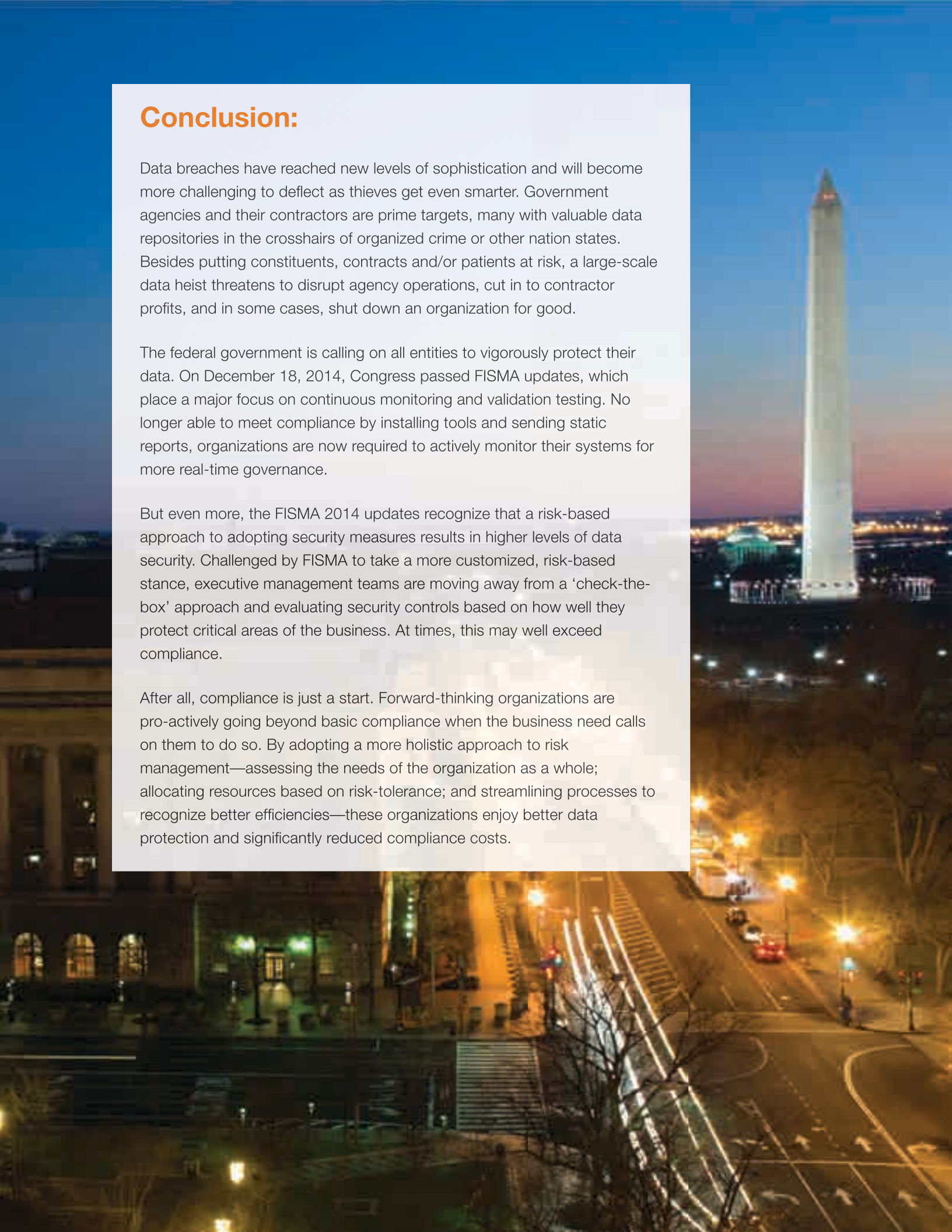
Third Party Assessment Organizations (3PAOs)

To help manage the complexities of moving to the cloud, many agencies, contractors, and CSPs engage a 3PAO. A 3PAO is an accredited independent assessor who can consult with you on the security implications of moving to the cloud. 3PAO's are the ones who verify that CSP's meet FedRAMP requirements when providers initially request certification, so 3PAO's have first-hand knowledge of how to assess a CSP's qualifications for you.

An overview of what you can expect a 3PAO to do for you includes:

1. Evaluate potential CSP for compliance with FISMA/FedRAMP
2. Support contract negotiations to clearly delineate responsibilities and expectations
3. Help classify the risk level of data
4. Structure a migration plan with regards to data security
5. Test and validate CSP security controls on an ongoing basis
6. Provide overall guidance, education, and support on adhering to cloud security best practices

If you are thinking of moving your data to the cloud, be assured that CSP's are constantly improving, as it's in their best interest to do so. Typically, providers invest in a physical and digital security infrastructure that most in-house IT departments can only dream of. They are subject to certifications and audits on an ongoing basis, and they often deploy advanced surveillance systems, data encryption, and regular testing against attacks. In other words, despite the fears associated with moving to the cloud, CSP's may eventually become the *safest* place for your data to reside.



Conclusion:

Data breaches have reached new levels of sophistication and will become more challenging to deflect as thieves get even smarter. Government agencies and their contractors are prime targets, many with valuable data repositories in the crosshairs of organized crime or other nation states. Besides putting constituents, contracts and/or patients at risk, a large-scale data heist threatens to disrupt agency operations, cut in to contractor profits, and in some cases, shut down an organization for good.

The federal government is calling on all entities to vigorously protect their data. On December 18, 2014, Congress passed FISMA updates, which place a major focus on continuous monitoring and validation testing. No longer able to meet compliance by installing tools and sending static reports, organizations are now required to actively monitor their systems for more real-time governance.

But even more, the FISMA 2014 updates recognize that a risk-based approach to adopting security measures results in higher levels of data security. Challenged by FISMA to take a more customized, risk-based stance, executive management teams are moving away from a 'check-the-box' approach and evaluating security controls based on how well they protect critical areas of the business. At times, this may well exceed compliance.

After all, compliance is just a start. Forward-thinking organizations are pro-actively going beyond basic compliance when the business need calls on them to do so. By adopting a more holistic approach to risk management—assessing the needs of the organization as a whole; allocating resources based on risk-tolerance; and streamlining processes to recognize better efficiencies—these organizations enjoy better data protection and significantly reduced compliance costs.

LBMC Security & Risk Services

LBMC Security & Risk Services understands how to implement and maintain compliance with security frameworks for the highly regulated Federal government contracting industry. LBMC has a dedicated practice team devoted exclusively to the issues facing government contractors and Federal agencies. Many of our team members have walked in your shoes and have worked as security professionals for organizations like yours. This perspective allows us to identify security issues in your organization more quickly. And our advice is practical and relevant to your environment and communicated in a way that is easy for executives without security expertise to understand. These practical solutions lead to real results and a tangible return on investment.

Government Security Services:

At LBMC Security & Risk Services, we have a solid track record of helping government contractors achieve compliance without compromising their growth and profitability. Our team of data security experts has in-depth knowledge of regulatory agency policies, business processes and cutting-edge data security solutions.

As part of our full suite of services, we offer:

- Independent Compliance Testing & Validation. Whatever your compliance need—FISMA or FedRAMP assessment to a SSAE16/SOC to a HITRUST CSF report—we take a practical approach that streamlines the process while allowing your organization to qualify for additional contracts.
- Audit Preparedness. We can also make sure your organization is ready for upcoming agency and customer audits. Drawing on our extensive compliance experience, we highlight the highest risks in areas where auditors are most likely to focus their scrutiny that will generate high risk findings.
- System security plan (SSP). We can develop or teach your staff how to create this document that describes how controls are applied and implemented to protect sensitive government data.
- Security risk assessment. We provide an independent, objective perspective on business and technology risks based on the stringent NIST 800-53 requirements.
- Penetration testing and vulnerability assessments. We identify and prioritize weaknesses through physical, logical and social testing techniques.

Ready to discuss your FISMA compliance concerns?

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