SANS

A SANS Whitepaper

How to Automate Compliance and Risk Management for Cloud Workloads

Written by **Matt Bromiley**

March 2019

Sponsored by:

AWS Marketplace

Introduction

There seems to be a constant battle between how fast businesses can grow and whether they can secure their customers' data. Many organizations get so wrapped up in trying to expand and scale for customer access that they make quick-fire, ad hoc decisions that negatively impact the security of the data of those very same customers. Complicating matters, the explosion of cloud-based services and offerings has led many organizations to quickly adopt services whose risks, quite frankly, they may not understand.

Of course, various compliance standards, such as PCI DSS and FedRAMP, have been developed to help organizations establish models to combat the loose handling of customer data. But this is where many organizations get lost. At the mere mention of the word "compliance," business and process owners tend to sink into an endless stream of acronym soup and never come up for air. But they do not have to fight this battle alone. The cloud is easy to deploy, but so is compliance.

While moving various elements of your business to the cloud does not remove the need for compliance, it does shape how you view, apply and assess compliance and risk management. In this paper, we focus on how moving to the cloud presents new compliance opportunities and how to seize them for your organization. We also examine a case study where a business has made a sudden shift to the cloud and look at some of the additional risk considerations it needs to make.

Last, we ask you to consider what may be a potential paradigm shift in how your organization approaches compliance and data security. In what we are calling "compliance-forward cloud planning," we encourage organizations to rethink the way they plan and deploy their cloud infrastructures, with compliance a focus from the beginning and not an afterthought. By focusing on compliance at the onset, organizations can make infrastructure decisions that will maintain compliance—not violate it.

Of course, if your organization has already moved to the cloud, compliance-forward planning may not be applicable, but the concepts pertaining to how to remain compliant certainly are. At the end of this paper, we hope you have some new thoughts and insight to bring to your team to discuss compliance and risk management options.

Compliance-forward cloud planning is the concept of making cloud infrastructure planning decisions based on adhering to compliance of data *first*—not as an afterthought.

Risk Management: Protecting Your Customers

Before we discuss techniques to secure your data and infrastructure within the cloud, it is important to understand how your risk model changes within the cloud. Some organizations think that because the data exists in the cloud—that is, on someone else's system—compliance is no longer their responsibility. This is not the case, and such an assumption is likely to put a business at risk.

When an organization takes advantage of services and/or infrastructure within the cloud, only a handful of responsibilities transfer to the cloud provider. For example, the cloud provider is responsible for ensuring that the network and hardware remain up and functional. However, the organization is still responsible for the security of the data that is placed within the cloud resources. Figure 1 illustrates the division of responsibilities between an organization and its cloud provider.

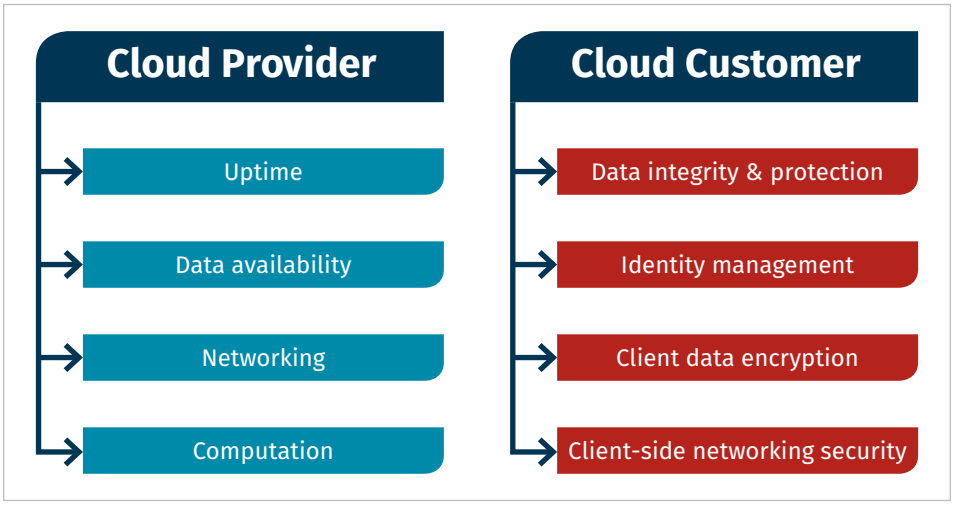

Figure 1. Respective Responsibilities of Cloud Provider and Customer[1]

Breaking Out of "Compliance-Backward"

As mentioned earlier, one of our goals with this paper is to shift to a compliance-forward frame of mind, where compliance becomes part of the design, not an afterthought or a nuisance. However, moving away from a compliance-backward approach is much easier said than done. Understanding compliance and what your data may be subject to can sometimes seem like a daunting task. In this section, we discuss common compliance standards and how to bring them into your organization.

[1] Note that your cloud provider may offer its own shared responsibility model. Check with your provider to verify what it does and does not provide.

Common Compliance Standards

Table 1 lists some of the more common compliance standards that your organization may encounter.

Table 1. High-Level Compliance Standards

Standard	What It Protects or Defines
FedRAMP	The approach for security assessment and monitoring that must be in place to provide services to the U.S. government
HIPAA/ HITECH	Standards for securing the privacy of protected health information (PHI)
ISO 27001	Standards for security management and program implementation
PCI DSS	Payment cardholder data (CHD) or data used in transaction authorization (sensitive authorization data)

Bringing Compliance into Your Infrastructure

Whichever compliance standards your data may be subject to, cloud infrastructure provides multiple ways to achieve compliance. One of the most apparent is the ability to make use of multiple third-party vendors. Furthermore, your cloud provider may offer native, compliant-ready solutions that, when coupled with third-party integrations, can alleviate a lot of compliance headaches.

Oftentimes, cloud providers facilitate third-party integrations and automations that allow for various application and infrastructure testing. Compliance is no different. Figure 2 describes techniques that you can use *today* to ensure your business remains compliant.

Automated Compliance Testing

With an automated infrastructure comes automated testing. You can select third-party providers and/or vendors to test your data on a frequent schedule.

Compliance testing can range from ensuring individual account access to validation that well-known encryption standards are in place.

Automated Vulnerability Testing

Vulnerability assessments and scans can be automated within the cloud to ensure that you are not exposed to known, widespread vulnerabilities.

Remaining patched from known vulnerabilities is your responsibility, as discussed earlier.

Compliance Scheduled Adherence

Unfortunately, many organizations do not scan or test their systems as often as they should. However, with data being accessible everywhere, you can schedule scans during convenient periods and ensure you are staying compliant.

The Benefits of Someone Else's Technology

While the cloud presents lots of challenges, it also presents a unique benefit in removing the technology "problem" from the organization.

By focusing instead on building secure applications, hardware and availability are cleared.

Figure 2. Techniques for Achieving Compliance

Case Study: Protecting Data on Multiple Angles

In recent years placing customer data within NoSQL and key-value databases has been a common strategy. With an easy-to-manage back end and rich front-end development options, NoSQL databases provide developers an easy-to-consume data format to enhance the customer experience. However, faster, compliance-second development also allows for compliance mishaps.

Let's examine an organization called "Bobby's Bits," a company that recently moved its infrastructure to the cloud. The following sections describe specific areas where compliance mishaps may negatively impact the organization and how to potentially mitigate or implement better controls.

Bobby's Bits: A New Cloud-Based Model

Bobby's Bits, a fictional organization, helps small businesses accept and process payments for online and in-store orders using payment methods other than cash or credit card. Bobby's business used to be fairly local, but because of some recent word-of-mouth marketing, the business has grown quite significantly. As a result, the owner had to hire a handful of developers and move his business away from the servers in his garage to the cloud. This move provided Bobby and the team easier access to all of the

business's resources and allows them to automatically scale for busy days. Figure 3 shows a high-level diagram of the new business structure.

With this new cloud-based model, the company can scale quickly to meet the demands of its customers—and the demands of its customers' customers. But this rate of growth could be creating a compliance risk. In the next section, we examine a few areas where Bobby should probably exercise caution and slow down (and where you should too!).

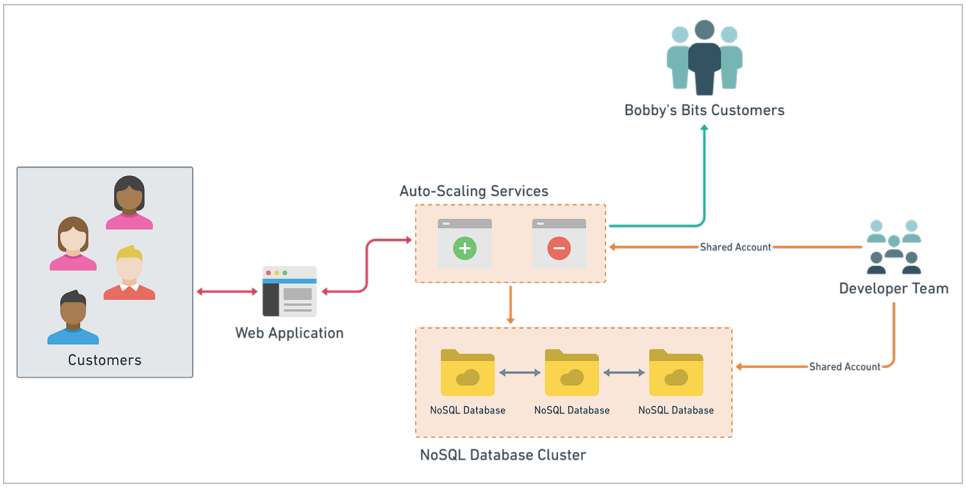

Figure 3. High-Level Diagram of the New Cloud-Based Model

Protecting PCI Data

The Problem:

Bobby is assisting his customers in facilitating payments for their customers. This is an immediate escalation in compliance requirements, because Bobby is inserting his business into the payment process, which contains sensitive, protected data (see Figure 4). Furthermore, Bobby is handling payments for multiple merchants, which means he must also be segregating *and* protecting data.

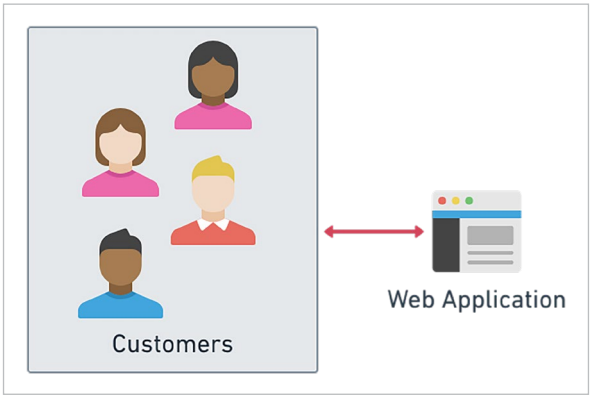

Figure 4. Customer PCI data within the organization must be defended.

The Fix:

During the development of Bobby's application and infrastructure, it is crucial that data segregation and encryption are in place. This approach will help him adhere to necessary PCI standards, as well as others concerning data integrity and confidentiality. Furthermore, when Bobby's customers come to request their data, he must ensure that no commingling is happening.

Unnecessary Data Exposure

The Problem:

Another issue that many organizations tend to gloss over is just how vulnerable they may be internally. To make life easier, when Bobby hired and set up accounts for his developers, he simply gave them all a shared administrative account (see Figure 5). Unfortunately, this is a dangerous practice that may result in security and/or data concerns.

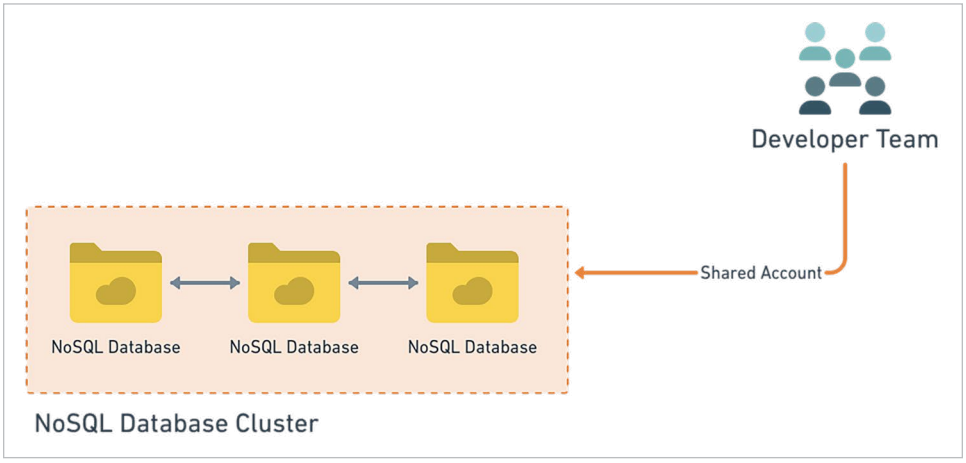

Figure 5. The development environment has potential data exposure.

Let's examine a few possibilities:

- The development team is likely working on the business during all hours of the day—and potentially on multiple devices. Bobby needs to gain insight into whether the data is being synchronized and/or used by his development team outside of his protected space.
- The sharing of credentials among the development team also poses a significant risk. For example, what happens when developers leave? Are their credentials changed?

The Fix:

Identity access management is one of the cornerstones of cloud infrastructure. For this reason, Bobby should take advantage of the robust authentication mechanisms put in place and ensure that his team uses unique credentials. Furthermore, he needs to ensure that users have *only* the privileges required.

Defaults Don't Always Help

The Problem:

One of the greater areas of risk that incident responders encounter as organizations deploy applications and solutions within the cloud is a reliance on technology defaults. Unfortunately, many applications are designed to be open sourced, hacked together and then secured by the organization itself. Many NoSQL solutions, for example, used to be available with ports open and available to the internet (see Figure 6).

In early 2017, this led to a massive global issue of data compromise and NoSQL databases being held for ransom.

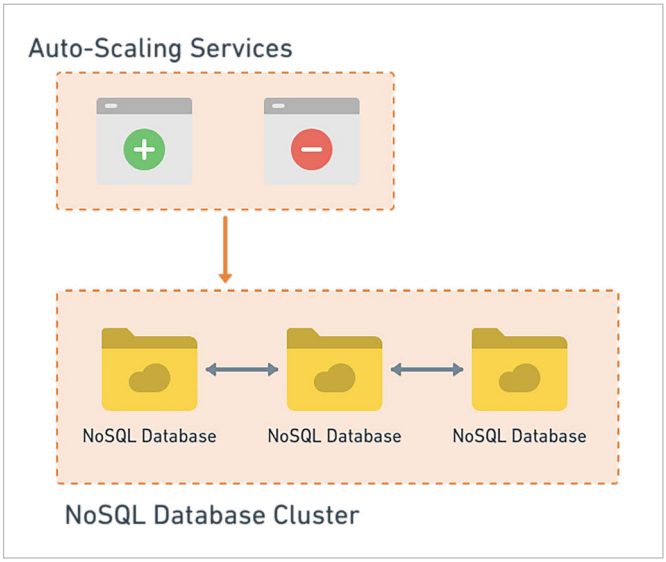

Figure 6. The use of default settings can put the organization at risk.

In Bobby's Bits, Bobby may not have hired the correct security personnel to help harden the various applications. Furthermore, if Bobby's development team simply was working on a fix, it may have inadvertently left default ports and/or default accounts open and accessible to the world.

The Fix:

The fix is twofold. First, Bobby and the development team should work to ensure that the various applications and tools they use are hardened by—you guessed it—compliance standards. This may include enabling encryption, setting up role-based access controls and limiting open ports/network routes to the application.

Additionally, with Bobby's infrastructure being in the cloud, he can resort to automated compliance scanning and verification tools. These scanning and vulnerability assessment tools will be kept up to date by the various vendors and can help ensure that the application is protected against the latest as well as pre-existing threats.

Furthermore, because Bobby's infrastructure is in the cloud, he can schedule scans much more frequently than some organizations like to do at the physical level.

Summary

Many decisions regarding data security and compliance are made utilizing standards set forth to help protect that particular content. Unfortunately, as organizations experience growth and network expansion, they often make decisions that may impact the safety and integrity of the data they store and use.

This is not an intentional mistake. Many organizations are growing exponentially and are seeking technology to facilitate that growth. This has driven a lot of organizations to the cloud—all in all, a great thing! The cloud can solve unique challenges of scale and availability—something very crucial to business. However, some organizations are also thinking that because the data is in the cloud, security is no longer their problem.

In this paper, we examined the concept of compliance-forward thinking, which asks organizations to consider compliance requirements when they are planning and building infrastructure, instead of afterward. There is a wealth of options within the cloud service space that can assist in automating and monitoring compliance of your organization and/or your customers' data.

As more organizations consider the options that cloud services can bring their business, it is crucial that compliance is at the top of the list of requirements. We have found that by starting the conversation with compliance in mind, what was once a tricky subject has become a guiding light to help organizations make safer decisions about the handling of customer data.

A few parting thoughts for organizations that are currently facing these issues head on:

- Look for areas within your cloud providers where compliance can be automatically monitored and/or reported on. Furthermore, look for compliant-ready deployments that can help fix requirements head on.
- Almost all compliance requirements include basic access rights monitoring, to ensure that employees are not sharing accounts and/or access mechanisms. If you set up individual accounts from the start, this requirement will already be fulfilled.
- It is easy to take newer technologies, drop them in place and begin working. But time and time again, we see organizations suffer breaches and noncompliance because of following the defaults. Make sure your team knows how to harden—and maintain—a good state of security within your applications and associated software.

About the Author

Matt Bromiley is a SANS Digital Forensics and Incident Response instructor, teaching Advanced Digital Forensics, Incident Response, and Threat Hunting (FOR508) and Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response (FOR572), and a GIAC Advisory Board member. He is also a principal incident response consultant at a major incident response and forensic analysis company, combining experience in digital forensics, incident response/triage and log analytics. His skills include disk, database, memory and network forensics, as well as network security monitoring. Matt has worked with clients of all types and sizes, from multinational conglomerates to small, regional shops. He is passionate about learning, teaching and working on open source tools.

Sponsor

SANS would like to thank this paper's sponsor:

aws marketplace