Delivering SOC 2 Compliance in the Cloud Post-M&A

7FACTOR

We Build Good Things

At a glance

When a publicly traded, multi-billion dollar automotive company needed help bringing an acquired company to compliance under SOC 2 guidance in the cloud, we put our extensive knowledge of AWS best practices to work. The client highly valued compliance and security practices and wanted to make sure that the acquired company would meet the same standards as the two joined together.

Using the AWS Well-Architected Framework, with its focus on operational excellence, security, reliability, performance efficiency, and cost, we conducted a thorough cloud-based assessment to produce a remediation list, then executed on it to create standardized, compliant and secure workflows across the newly expanded business.

AWS Cloud | AWS Well-Architected Framework | Compliance Audit | Automotive Industry

Key Insights

Remediated over **50+** **Security** and **compliance** issues across three different departments

Provided and led **SDLC training** to **three key** departments

Consolidated and restructured **three disparate enterprise systems.** Including **source control, ticket management, and change control management.**

Remediated issues across **6 AWS accounts**

Ensured **AWS best practices** were adhered to while executing **well-architected reviewed assessments**

Background

Cybersecurity is top of mind for M&A

Any time two businesses become one, their systems have to connect—which automatically introduces security vulnerabilities under the best of circumstances. Growing awareness of this issue means sometimes a deal can't go through without quality assurances around cybersecurity and proper treatment of data.

According to a study conducted by Forescout, 53% of survey respondents indicated that cybersecurity issues have threatened their M&A deal negotiations.[1] Additionally, the acquiring entity has to think not only about the security posture of their acquisition, but also how that company's vendor network could introduce new threats, depending on the level of established governance and risk mitigation that shapes those relationships.

Integrating different systems into one also forces modifications for end users across systems, tools and processes, introducing another layer of potential security concerns. Humans are fallible, after all, and tend to cause the lion's share of security issues. Case in point: a study by Stanford University and Tessian concluded that 85% of all data breaches are caused by an employee mistake, and 43% of people have made errors that threatened their company's security posture while at work.[2]

The good news is, most major enterprises are paying attention to the security complications attached to M&A deals. Deloitte projected that in 2022, 60% of organizations would factor cybersecurity directly into the due diligence process.[3]

SOX, SOC & the compliance question

On top of the concerns around security, there's also the question of compliance. When a new business joins yours, you need to make sure their practices comply with relevant industry standards and regulations to avoid hefty fees and protect your brand reputation in the long run.

One such standard is SOX, legally mandated by the Sarbanes-Oxley Act, which was passed in 2002 as a response to a string of financial scandals involving corporate giants like Enron and WorldCom. Designed to restore public trust in financial reporting and corporate investment, the standard focuses on creating internal controls for financial records, as well as systems of accountability for executive leadership. CEOs and CFOs, for example, are required to attest to the accuracy of records.

In a nutshell, if your company touches money, you're obligated to comply with SOX. It includes provisions for public and private companies that require them to create processes for storing, protecting and ensuring the accuracy of financial information.

Background

Key functional areas of SOX compliance include:

- Access controls
- Security & cybersecurity
- Segregation of duties
- Change management
- Backup systems
- Disaster Recovery

A word of caution on compliance

A common misperception of SOC standards is that they are an all-encompassing analysis of cloud security, but that's not the case. SOC is a standard for managing the integrity and confidentiality of data: a critical dimension of security, but by no means the totality of all cloud security concerns. You need to take a holistic approach in any audit to fully address both SOC compliance *and* all cloud security concerns.

Another important set of standards for any service organization is System and Organization Controls (SOC), which includes three types. SOC 2 requires a third-party audit to assess five areas related to managing customer data: security, availability, processing integrity, confidentiality and privacy. Although the standard is not necessarily required in most industries, it has quickly become table stakes for any reputable company that manages customer data.

Solution

For us, compliance is the main dish

The team at 7Factor was uniquely positioned to carry out an effective security audit for this client because of our extensive experience building applications in the cloud. We routinely own all aspects of an application's lifecycle, including network segmentation, all the way out to deployment using CI/CD systems.

We also designed our internal software development lifecycle from its inception to be SOC compliant. In other words, for us, security and compliance are not afterthoughts that get added on after the fact. A compliant workflow structures everything we build, so we know it well.

Well enough, in fact, that we're able to advise clients on the state of their existing environment with greater insight and precision. Because our engineering managers understand how to implement and execute a compliant workflow, it's easy for us to walk into a non-compliant one and identify the problems with it. And because we've built environments from scratch that have withstood SOC audits, we can identify issues with a client's continuous delivery of infrastructure into the cloud that much faster.

We have practical experience with third-party audits of major enterprises, having recently concluded a SOC audit for a multibillion-dollar publicly traded healthcare company. We also regularly develop custom solutions for clients in critical industries required to comply with standards such as HIPAA and PCI DSS.

The audit begins

Armed with extensive knowledge of both SOC and SOX requirements, we began the audit. With compliance as our guide, we also factored in additional security concerns so that our recommendations would provide holistic risk mitigation. As a best practice, our team starts with read-only access to the client's account so that we can focus on assessment, then requests administrative access to execute on the remediation plan. When conducting an audit, we start with the infrastructure to get a general sense of what's wrong. We also identify issues that are not infrastructure-related: problems rooted deeper in the application code.

Solution

By starting at the cloud level, we keep our attention on methods of deployment and only engage source code where needed. Within the SOC framework, what's important is not so much the source code itself but rather who releases it (and how). SOC 2 calls for a separation of controls, meaning the person who builds the code should not be the person who deploys it. Given our experience building applications in Fintech, healthcare IT, aviation, and other highly regulated industries for over six years, we're well acquainted with how to comply with such requirements using continuous delivery, which relies on automation for code deployment.

We divided our findings into two categories. The first covered general hosting and security best practices for applications running in the cloud, incorporating best-in-class cloud architecture techniques and standard operating procedures regularly implemented by software engineering organizations. The second honed in on data security, backup, and disaster recovery, covering practices and recommendations for maintaining SOC 2 compliant persistence stores. At the end of the document, we provided a general rubric for the health of the account compared to a compliant implementation.

Compliance in the cloud is different from on-prem

One challenge with this particular audit was that the newly acquired company operated in a cloud environment. While the client had perfected its on-prem compliance and security practices — and has experience using secure cloud services for some functions — the acquired company's fully cloud-based environment would need to fold into their primarily on-prem processes, introducing new considerations and practices that we needed to highlight and correct for.

> "Don't put everything in serverless. There are some things that you keep. That's why I appreciate services like Amazon Elastic Container Service (ECS). It requires you to run machines and keep them patched but you can still deploy containerized, modern applications. There are capabilities inside Amazon to do that for you, but you have to set these up correctly."
>
> **Jeremy Duvall**
> *7Factor Founder*

A key consideration for this type of audit is that cloud compliance works differently than on-prem, so it's crucial for the auditor to understand how compliance guidelines apply across both types of environments. For example, in an on-prem environment, SOX guidelines stipulate that you must physically manage and guard your servers. You're also responsible for a slew of management tasks including host operating patching, operating system patching, user provisioning and de-provisioning, and domain administrative accounts.

But the cloud has redefined the paradigms of how a data center works. Major public cloud service providers like AWS operate on a shared responsibility model in which a portion of the on-prem responsibilities no longer apply.

Solution

“50% of the old way still applies. The other 50% doesn’t because access control is managed by the cloud provider’s platform,” 7Factor CEO Jeremy Duvall explained. When using serverless services like Fargate and lambda, the client is no longer responsible for managing the environment like they would if it were their own. Does that mean a company should go entirely serverless? Not necessarily.

“Don’t put everything in serverless,” Duvall added. “There are some things that you keep. That’s why I appreciate services like Amazon Elastic Container Service (ECS). It requires you to run machines and keep them patched but you can still deploy containerized, modern applications. There are capabilities inside Amazon to do that for you, but you have to set these up correctly.”

Results

Risk mitigation is the end target

Moving from the start of the audit to the final items on the remediation list took about ten weeks total. In the end, we were able to help the client spot and resolve potential compliance and security concerns as they acquired the new company. We also emphasized the need for standardization to a single, compliant practice for all software teams throughout the process.

In the short term, the SOC 2 compliance audit will help them avoid any penalty fees that stem from violating regulations like SOX or PCI DSS. In the longer term, our dual focus on compliance and security puts the client in the driver’s seat when it comes to risk mitigation. By fixing the smaller issues up front, they reduce the possibility of a bigger problem down the line in terms of data breaches, ransomware, malware—and whatever new threat is right around the corner.

We Build Good Things

Let us **show you how**

7FACTOR