Alliant®

The Journey to SOC 2:

Data Security Lessons and Benefits

by
Nicholas Godlove
Corporate Counsel, Alliant

SOC 2 AUDITED TYPE I

SOC 2 COMPLIANT TYPE I

PART 1:

A New Link in the Secure Data Supply Chain

Alliant recently received SOC 2 attestation for its real-time consumer data systems. The audit procedures by an independent third-party accounting firm were challenging, costly, and time-consuming, but ultimately rewarding.

The process involved multiple subject matter experts working laterally across Alliant's business units. The reviews were rigorous, with extensive documentation requirements, but in the end, the process was valuable and the entire company developed a heightened awareness for security policies and procedures. It helped Alliant reaffirm across teams that data security and integrity is a competitive advantage — and the process itself challenged each team to actively think about and defend its data practices.

After a six month effort, Alliant is now a certified member of the secure data supply chain. Information entrusted to us from our cooperative members and partners is confirmed to be held securely and processed correctly.

Data and analytics information is sensitive, and Alliant believes that all data providers should be on the vanguard of obtaining security certifications — and should seek out partners that do likewise. This is a conversation management in every company that relies on consumer information to conduct business should be having. And if you're thinking seriously about putting your company through an information security audit, we are confident that the lessons we learned can help you too.

Information entrusted to us from our cooperative members and partners is confirmed to be held securely and processed correctly.

***What is SOC 2?**

SOC 2 is an auditing procedure that ensures a service provider securely manages data to protect its clients. For security-conscious businesses, SOC 2 compliance is a mandatory requirement when considering a service provider. The SOC 2 standard is based on the criteria outlined in the Description Criteria authored by the AICPA, the American Institute of Certified Public Accountants.

PART 2:

Which Data Security Standards are Right for Your Organization?

Just a few years ago the only companies that took the initiative to prove their cybersecurity credentials, generally, were the ones required to by law. However, in the past three years, companies in the SaaS, consumer data and marketing sectors have come under increased pressure to document and certify their information security practices to outsiders.

Organizations are increasingly evaluating whether they should attempt to become certified or accredited, even if they are not under statutory or contractual obligation to do so. Obviously, organizations that are required to comply with HIPAA or PCI understand the obligations. This year — no matter what sector your company operates in — if you hold consumer information for marketing and/or operating purposes you should consider whether some kind of cybersecurity accreditation would be a worthwhile corporate goal.

The next question concerns the auditing and certification framework that's right for your company. Management should work with qualified counsel to define critical needs. However, some basic questions to ask include:

- Are we fully compliant with existing legal/contractual requirements such as Dodd-Frank, PCI, HIPPA and GDPR? Are we prepared for upcoming regulations such as CCPA?
- Which information assets are critical to the business and warrant security investments?
- Which business units handle sensitive or proprietary data that should be audited?
- Are our current practices sufficient to obtain certification in all areas?
- What reps and warranties concerning data security are our clients and partners likely to require?
- What are our risks? Could our organization afford to pay for breach notifications required by law or survive a lawsuit resulting from an unreasonable cybersecurity posture?

There are different standards that focus on the ability of an organization to identify threats, protect itself, detect attacks, respond to incidents, and recover from them. Because these factors are the first line of defense, every cybersecurity standard covers some combination of them.

Alliant chose SOC 2, an accounting standard formulated by the AICPA. Another popular standard is the ISO 27001 framework, which is part of the ISO/IEC family of supply chain quality assurance. ISO/IEC is well-respected internationally. If you are doing business internationally or want to seek EU partnerships, you may want to evaluate the ISO 27000 framework.

Another popular protocol you may want to consider implementing is the NIST Cybersecurity Framework. This standard is published by the federal government and designed to provide easy to use guidance for business and other private organizations.

It is increasingly unreasonable to expect to hold consumer data without having the resources to protect that information. If your company routinely manages data for clients and other third parties, you should absolutely commit resources to assure your place in the secure data supply chain. Data resellers, analytics companies, digital publishers and advertisers, and others that use or rely on consumer data should all be prepared to validate their cybersecurity procedures, even if data is not your company's primary business function.

It is increasingly unreasonable to expect to hold consumer data without having the resources to protect that information.

PART 3:

Benefits and Challenges on the Road to Peace of Mind

Most certifications entail a two-step process. First your organization goes through an audit by an independent professional. Then, based on the results of that audit, your team addresses any identified issues and prepares for the appropriate certification.

An immediate benefit of the audit process is peace of mind. Without that scrutiny, it can be difficult to ascertain what you don't know about your information assets. What are your crown jewels? Where are they located? Who can access them? Many organizations are surprised when they systematically dig through their data flows and comprehensively answer these questions for the first time. The process of compiling the information and ensuring that your organization will be ready to deliver the required documentation to an auditor is a big task, and one that can be useful internally.

The audit and test processes that are part of certification deliver valuable insight that bring clarity to your data handling processes. Consider the value of being able to:

- Produce a comprehensive data-flow diagram
- Document all procedures that allow access rights to valuable IP
- Expose a potential network weakness after a third-party penetration test or regular vulnerability scans

Management buy-in is critical to successfully earning certification, because you're going to need to justify significant time commitments, and potentially expenditures, from your network and IT staff — reviewing standards, producing logs, and validating processes. And the number of departments touched by any of the cybersecurity standards far exceeds just your IT team — HR, finance, legal and compliance, and even sales all have a role to play. Trainings, new security requirements, and reductions to data permissioning will all demand time.

Without certification, your organization will struggle to answer basic questions about your cyber-defense posture. The risks an organization is taking regarding its networks, intellectual property, and consumer data, are largely unknowable before it completes its first audit. And the potential effects of not knowing can be catastrophic for your organization.

After having completed the audit, Alliant can attest that the rewards are well worth the effort.

PART 4:

Benefits of Achieving Data Security Certification

Achieving certification is not something an organization can do once and then rely on forever. It is an ongoing commitment to data security, integrity and privacy that must become part of the culture of your company.

Compliance with standards must be documented and withstand annual audits. Changes to the network must be evaluated and tested. New bugs and vulnerabilities in software must be fixed. New requirements must be accommodated, forever. It all requires ongoing effort and material investments.

Ultimately, though, this is the right choice — if your organization intends to retain the privilege of accessing and maintaining consumer data. At Alliant, we consider our security to be foundational investments for being a trusted link in the secure data supply chain.

There's no way around it: obtaining a qualified third-party auditor is difficult, and not inexpensive. Beware auditors that "align" with ISO standards, or auditors that will "review" your policies and proce- dures. You need to find qualified auditors that are certified to review the standard you are looking for. If you want to become SOC 2 certified, for example, you need an accounting firm to audit you.

Companies that document their security posture are well-positioned in the current marketplace to meet evolving client requirements. Since data owners can be held liable for vendor negligence in handling confidential data, entrusting PII to a third-party without data protection measures can embroil them in regulations and lawsuits. For this reason, many organizations are requiring that other companies handling their data demonstrate objective proof of reasonable cybersecurity measures.

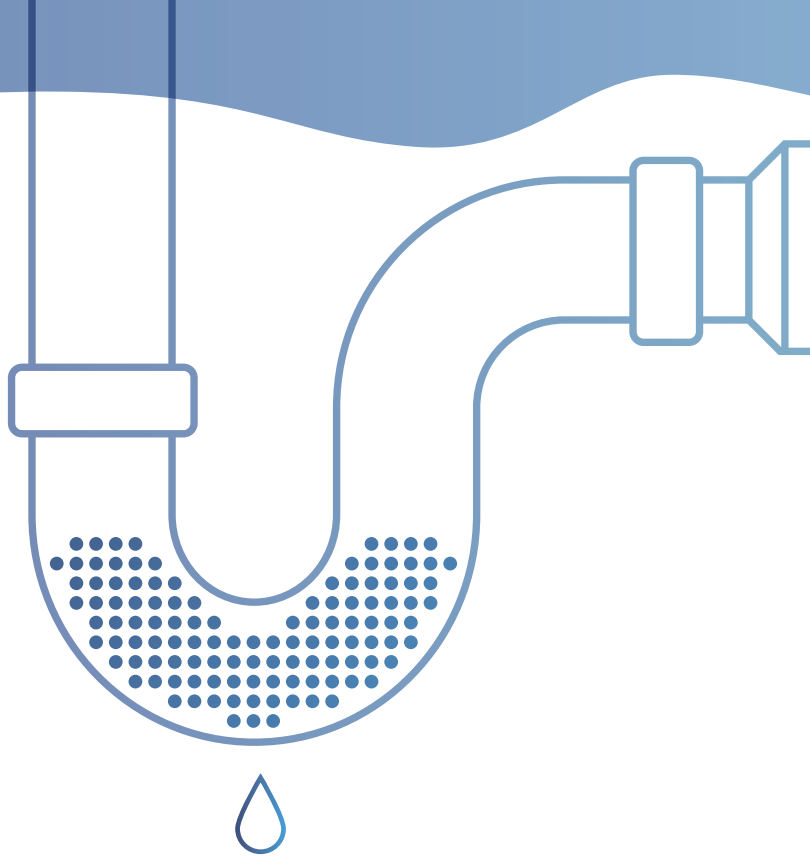
KEY BENEFITS

- **Minimize susceptibility to data threats and create the systems to manage them**
- **Increase organizational education and awareness that creates a culture where data security is paramount**
- **Differentiate your company from those who do not prioritize data security – which is valuable positioning in today's environment**

Consumers and lawmakers are also, rightfully, concerned about mismanagement of personal information. There will likely be more lawsuits and more laws in 2019 related to privacy, information disclosure, and breaches than in any prior year. Companies that audit their data flows will substantially reduce their chances of a breach, and will be able to provide evidence of reasonable security practices. These companies will also gain a head-start on new compliance regulations, as compared to companies that are waiting for regulators to define minimum legal standards.

It is clear that enough companies are taking privacy and data security seriously enough that we are going to see a "new normal" in 2019. Companies that take cybersecurity seriously will band together and keep data in the secure infrastructure, while companies that are not continually improving will find themselves shut out and left in the cold with their businesses severely compromised. Sharing information with organizations that cannot reasonably safeguard that information will further be seen as unreasonable, on par with failing to lock the building doors at night.

As companies that can trust each other band together, highly secure information sharing and security practices will increasingly become the norm. If your organization wants to be a part of this 21st century transformation, you'll need to prove you can play. In the digital age, leaky pipes can affect the entire pipeline. And those that won't shape up will be cut off.



In the digital age, leaky pipes can affect the entire pipeline. And those that won't shape up will be cut off.

Conclusion

This is my perspective, from having shepherded the organization I work with through an audit. It was a rewarding experience, both professionally and personally, to ensure that the information we keep on behalf of our clients is objectively secure. We may not be required to reach these standards, but the people I work with were happy to push themselves to reach them. We all take our responsibility to the data seriously. If you feel the same way, or have questions about the process, please contact me. I'd be happy to answer any questions you have about the process or the results.

Nicholas Godlove, *Corporate Counsel, Alliant*
(845) 617-5482 | ngodlove@alliantinsight.com

Nick came to Alliant after a successful career in private practice advising technology companies on privacy and contracts. He is deeply involved in Alliant's data security and consumer privacy efforts. Nick earned his law degree at UC Davis and holds a Masters in Cybersecurity from Brown.