number8

UNDERSTANDING THE IMPORTANCE OF SOC COMPLIANCE & SECURE DATA MANAGEMENT WITHIN CONSULTING ORGANIZATIONS.

- OLIVER RAY, MANAGING DIRECTOR @ NUMBER8

When companies begin a vendor selection process they are typically attempting to find the best solution to a significant list of complex priorities. They're also considering the core principles of their organization. Chief among these principals is most often a commitment to developing secure, consistent, and high quality applications for their customer base.

Recently, the media cycle has been dominated by technology organizations that have run into privacy, security, or ethical incidents that fracture public trust. Oftentimes, these fatal organizational issues can be traced to shaky security related to processes, development, or technology selection.

There's no reason to slow down your development cycle to support a vendor who is not willing to do everything in their power to make your data and products secure. Securing your future development against the types of problems listed above, begins with the number8 SOC Consulting Services Delivery Model. Following this model ensures that number8 is a plug-and-play partner able to get your development team up and running with remote resources as securely and efficiently as possible.

ESTABLISHED SECURITY FROM AN ESTABLISHED TEAM

At number8, we have always believed that taking care of the fine details from the beginning ensures big things happen quickly and easily during delivery. In fact, that has become the foundation of our security philosophy. A long-term outlook on even our smallest projects paired with our consultants' long-term commitment to professional development has resulted in an ability to provide extremely secure processes to our clients.

Meaning, we treat your security like it's our security.

We've also recently formalized our commitment to these practices by establishing our SOC 2® report.

We believe the standards and controls framework established by the AICPA to become a SOC compliant organization match closely with number8's corporate values. Our approach to establishing a consistent, secure, and auditable delivery model empowers our commitment to creating high-performing, distributed agile teams.

WHY SOC 2?

Companies around the globe have shifted to the cloud as a way to increase flexibility, unlock growth, and reduce costs. However, that shift has also created an additional list of required considerations to deliberate before any new initiative is undertaken.

For example, both consumer-facing and B2B companies have to weigh the risk of moving customer data to the cloud versus their current security processes and protocols. Data breaches have become commonplace, leading to more critical questioning about software development initiatives across all organizations.

Decision makers must also weigh the benefits of the cloud's latest suite of tools that help make development easier for engineers. It is incumbent upon them to find the right ways to implement their patterns and practices to make initiatives successful.

This is where the SOC 2 comes in. As companies move to the cloud, bad actors have followed in droves causing costly breaches that have result in enormous fines, tarnished reputations, and high customer churn.

Protecting critical systems is important for all companies, certainly. But in specific industries like banking, healthcare, and software-as-a-service (SaaS), security needs to be a daily imperative. Actively protecting against threats in these fields can become a full-time job, which is why many of these companies are turning to the SOC 2 report process when certifying vendors to work with.

THE REPORT

The SOC 2 report is intended to meet the needs of a wide range of users that require detailed information, testing, and assurance about the controls at a service organization relevant to security and availability. These reports can play an important role in:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

The SOC2 report has focus areas across 5 main categories:

1. **SECURITY** — Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity's ability to meet its objectives.
2. **AVAILABILITY** — Uptime is maximized to eliminate as much waste as possible from tasks that do not move the business forward.
3. **PRIVACY** — Personal information is collected, used, retained, disclosed, and disposed of properly.
4. **CONFIDENTIALITY** — Information designated as confidential is protected.
5. **PROCESSING INTEGRITY** — System processing is complete, valid, accurate, timely, and authorized.

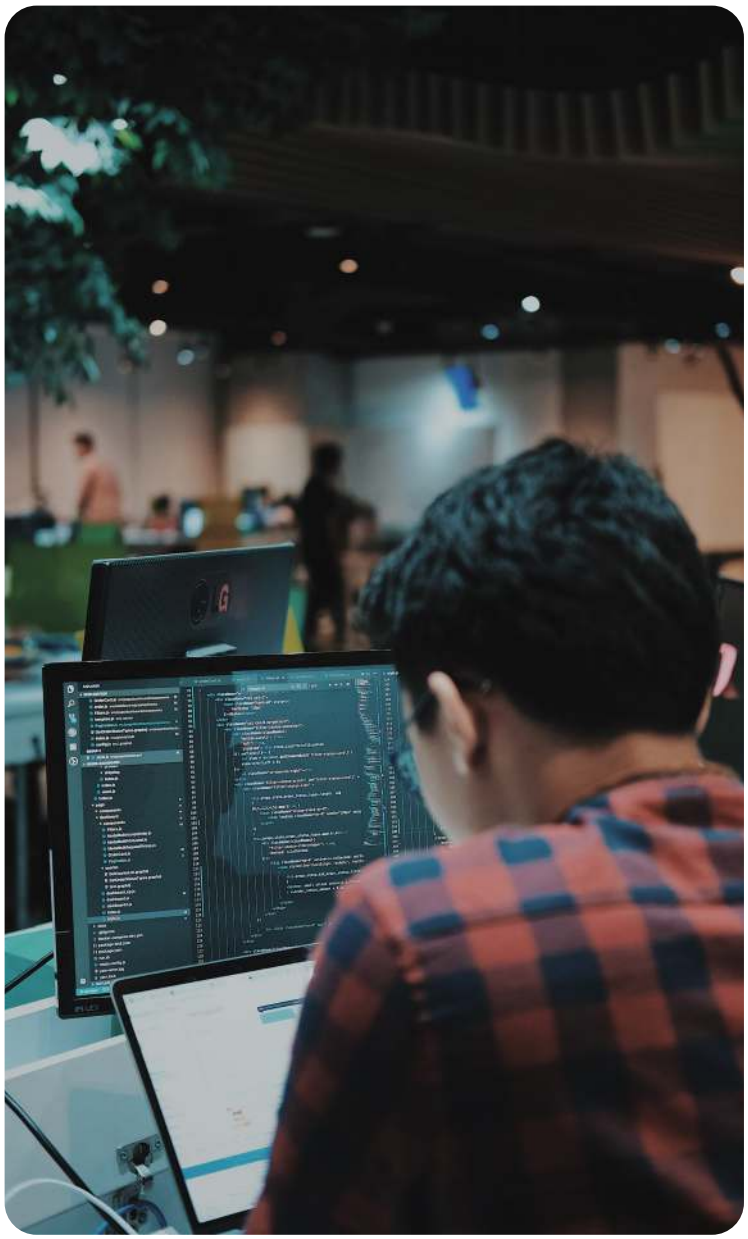
SOC TYPE 1 VS. TYPE 2

There are two categories to SOC 2 reports: Type 1 and Type 2.

Type 1 reports focus on management's description of the service organization's system and the suitability of design controls. Type 2 reports use that same information but also incorporate the design controls' operating effectiveness. On top of that, they review and provide assurances over a specified period.

Overall, Type 2 reports provide more information over how well controls work as well as give insight into how well a service organization maintains their control effectiveness.

IMPLEMENTATION



Our team at number8 takes an evolutionary approach to our delivery model. Meaning, the process is designed to fit the needs of every client and grow over time, because no two clients are the same and business needs change constantly.

We communicate with each client regularly to figure out the best way to engage with leadership, the development team, and the compliance department. It is a deeply interactive process that ensures we are exceeding the needs of each stakeholder within an organization.

Establishing an agreement to work with a client is just the beginning. Each conversation afterwards is part of a bigger picture. Quarterly, we review the happenings of the previous quarter with all levels of an organization. This process illustrates the successes and the points of improvement that can be made along the way and shows no conversation with number8 is isolated.

This review process is a direct result of number8's focus on business continuity. Above all things, we cannot be successful with a client unless we can guarantee that the work, and those individuals responsible for the work, are fully committed and consistent. We spend a considerable amount of time thinking through the potential risks, hurdles, and opportunities inside and outside of each account, and although we expect our consultants to be superheroes regularly, we establish check-ups along the way to help us focus on larger goals and make failsafe contingency plans just in case something goes wrong.

No matter the circumstance, the number8 priority is to keep delivering for our partners regardless of the environment around us.

The last foundational piece of our SOC 2 approach to nearshore development is the secure working locations of our delivery centers. Located in San Jose, Costa Rica and San Pedro Sula, Honduras, these facilities provide the type of security protocols that enterprise compliance departments would expect to see from vendors. For us, they provide much more than just security. They give our consultants the opportunity to gather and collaborate on the biggest challenges thrown their way, helping us better serve you.

STILL HAVE SECURITY QUESTIONS?

LET'S SCHEDULE A CALL.

CLICK HERE TO CONNECT

number8

Develop Without Limits.

Visit us at www.number8.com | Email info@number8.com | Call (502) 212-0978