eBook

The Complete Guide to SOC 2 Automation

GlobalDots

Intro: Compliance as part of the new cloud security stack

Security compliance is a necessary evil that's becoming more relevant than ever. Whether you're a B2B company and would like to sell your services to large enterprises, financial institutions, healthcare and public sector organizations, or you're a B2C company and must store and protect your end-user data, you must consider security and privacy compliance in your product design process.

Security and privacy requirements are articulated in various security standards. The most common ones include PCI-DSS, ISO-27001, and SOC2. For specific industries and service providers, additional regulations and standards might apply.

Your cloud security stack should therefore include up-to-date, compliance-friendly solutions. This usually means 1-click reporting, which generates the documentation qualifying as "evidence" to a certain standard's checklist. By implementing compliance-friendly solutions, companies can acquire compliance evidence faster with fewer efforts involved.

But that's not it.

The cloud's threat landscape changes almost daily. Therefore security standards, too, undergo constant updates, and new, additional ones emerge. This means soaring complexity which has to be managed, without interrupting core business processes such as product development and activity scaling. Having an automated, consolidated source of truth for compliance, where checklists are generated and evidences are automatically retrieved, becomes an acute need.

The words "SOC 2 Audit" might make you flinch. In this guide, we'll walk you through the best way to successfully prepare for—and pass—your next InfoSec audit and all future ones as well.

Introduction to SOC 2

SOC 2, designed to demonstrate that a business is doing everything in its power to protect and secure customer data, has become one of the most important compliance frameworks today. Developed by The American Institute of Certified Public Accountants (AICPA), SOC 2 applies to nearly all businesses collecting, storing, and sharing customer data.

While complying with SOC 2 is optional, there are major costs associated with failing to comply; many businesses won't consider working with companies that aren't audited for SOC 2, as this may indicate that the company is not yet mature in its internal security operations or that security isn't a priority for them. And accordingly, complying with SOC 2 shows potential customers and vendors that security is of paramount importance.

SOC 2 is based on AICPA's 5 Trust Service Criteria (referred to as the TSC). These are:

Security

How the business protects data, systems, and networks from breaches and attacks.
This is also referred to as the Common Criteria, the most prominent—and only required—section of any SOC 2 audit.

Availability

How the business ensures the uptime of systems.

Confidentiality

How the business ensures that any data it holds remains confidential.

Processing Integrity

How the business ensures that processing is, in the words of the AICPA, complete, valid, accurate, timely, and authorized.

Privacy

How the business collects, uses, shares, stores, and deletes personally identifiable information, or PII.

While only the Security Criteria is required, many potential customers and partners may require other criteria to be met as well. It's up to each organization to determine which criteria are most important to meet, usually based on the services in scope, and this is why no two audits will be exactly alike.

Prepping for SOC 2 Audits

To meet SOC 2 effectively, organizations must establish security policies that cover their chosen Trust Criteria(s). Organizations spend months in the preparation stage, understanding which systems should be included, establishing new policies and procedures, and working on improving existing ones. On top of that, preparing for SOC 2 requires all hands on deck; multiple stakeholders, across varying departments, must uphold practices and methodologies in order to achieve compliance.

Automation in SOC 2 Prep

As important as it is to achieve SOC 2 compliance, the manual work involved, along with all the minutia required, often leaves CISOs and Compliance leaders feeling overwhelmed at the prospect of preparing for audits.

But preparing for, and ultimately achieving, SOC 2 compliance doesn't need to be complicated or overwhelming. For too long, compliance has been trapped in the past, even while other industries have evolved through innovation. Today, organizations are starting to understand how automation can streamline and vastly simplify the audit preparation process.

Introducing Compliance Automation Platforms

This emerging category of SaaS solutions helps you preserve an ongoing status of compliance. This, thanks to 2 main traits:

Automated checklists

These platforms are synced with the latest versions of multiple frameworks. To-do lists are therefore automatically generated, to help both the project owner and the auditor check all items needed for certification.

Automated evidence gathering

Integrated with the business applications which produce the evidence, the Platforms are much more than just a secure, organized storage space. They actually produce and update the evidence with little to zero human intervention.

What Makes an Effective Compliance Solution

01

Continuous Evidence Collection

Automatically collect the required data from the enterprise apps and systems and organize them based on the compliance standard's format. Traditional evidence collection for compliance purposes is done in one point in time, which should be repeated upon recertification. Continuous evidence collection ensures the freshness of the compliance status of the company.

02

Relevant Standards Covered

Compliance Platforms is an emerging category, with lots of competition coming in as we speak. Know which InfoSec security standards you are subject to, and make sure your selected vendor supports as many of them as possible. The most commonly covered ones are SOC2, PCI DSS, and ISO 27001. According to your industry and geos of interest, you might be subject to others, such as HIPAA, ITGC, CSA, and more.

03

Easy Integration

As with many SaaS-based products, this one is a key to achieve customer adoption: both in terms of the effort to integrate the service and the number of enterprise applications supported. It should take less than a few hours to integrate and should include integrations to most common apps and systems out of the box.

04

Compliance Scoping Guidance

The compliance project owner is guided how to even start the compliance process, which teams should be involved, what type of evidence should be collected and in what format, etc. This capability is valuable for startup companies getting started in the compliance process for the first time, or more mature companies trying to tackle a new type of compliance standard.

05

Gap Analysis & Roadmapping

A holistic view on the company's compliance status on a daily basis, helping already-compliant companies remain so as they prepare for their external audit. Once most of the compliance related data is collected, a gap analysis is produced in form of a to-do list. This includes any recently-created gaps due to changing environments and configurations.

06

Auditor Communication Simplified

No more endless emails or chaotic shared drives. The auditor is given access to the platform, where they can review all evidence and comment in one organized place. This allows for the entire audit to be managed in the platform, with nothing lost or left unhandled.

7 Ways Automation Takes the Frustration Out of Meeting SOC 2

Saves money, time, and effort

The costs of hiring SOC 2 consultants, plus the months of effort dedicated to evidence collection, divert time, budget, and skills that could have been put towards core business functions. Automated evidence collection dramatically reduces costs and time-investment associated with SOC 2 prep, so businesses can focus on primary goals and KPIs.

Prevents errors

Manual processes breed mistakes and in the typical audit preparation process, there is a lot that can go wrong. Automating the evidence collection process prevents the errors that lead to audit failure from creeping in. And with automated data-to-control mapping and collection capabilities, teams always have the information needed and their evidence always fulfills requirements.

Removes dependencies and prevents audit fatigue

Prepping for an audit is a giant team effort, requiring compliance teams to repeatedly badger stakeholders for crucial information. This places a continuous and significant burden on these stakeholders, cementing SOC 2 in their collective mind as an impediment to innovation and productivity. Automating evidence collection removes dependencies—and therefore frustration—enabling compliance teams to prepare for audits, without the need to rely on, and continuously bug, others.

Negates the need for consultants / specialized skills

Typically, organizations need to bring in outside consultants to understand the meaning behind complex requirements. With advanced automation, there's no need to understand specific clauses or hire a consultant to explain them. Out-of-the-box control translation and effortless mapping make understanding requirements easy.

7 Ways Automation Takes the Frustration Out of Meeting SOC 2

Enables data-based risk analysis

When dealing with assessments, understanding gaps can help to analyze risk, and accordingly, determine how to handle it. When evidence is collected automatically, based on true data, it's always available, self-explanatory, and easy to understand and see any gaps, leading to faster remediation.

Provides secure data access

In order to collect evidence, access must be granted to the systems where the data resides, whether in read-only format or full-access format, for those involved in audit prep and the audit itself. But problematically, this means more people can access sensitive systems. With automating evidence collection, human access to data isn't needed at all. Instead, machine-to-machine access is granted via secured APIs, which provides a high level of segregation of duties, wherein even the Compliance Manager doesn't need access to the systems, resulting in enhanced security posture.

Simplifies adoption of additional frameworks

Once an organization has managed to pass SOC 2, they'll likely need to start all over again, when they need to adopt ISO 27K, PCI, etc. Or perhaps SOC 2 isn't their first compliance framework and they already have others in place. Automation makes it simple to establish a unified list of controls, which is already mapped to each of the frameworks relevant to the organization to easily meet new requirements.

Summing it All Up

Achieving SOC 2 compliance is no small undertaking, but it is an important maturity benchmark, signifying that security posture is a core value to your organization. Incorporating automation and innovation into the evidence collection process gives organizations the boost needed to seamlessly and efficiently meet SOC 2 and any other frameworks. Now go find your automation solution so you can finally Enjoy Smart Compliance.

Achieve Compliance Automation with Ease

Contact GlobalDots for wholesale pricing and full expert integration of the latest Compliance Automation Platforms.

About GlobalDots

GlobalDots is a 17-year world leader in cloud transformation, connecting businesses with the latest cloud & web technologies.

We consult, resell, integrate, and customize full-stack solutions, including: security, cost & performance optimization, connectivity, and managed services. Thoroughly studying and testing innovative solutions for today's security & business challenges, we only curate in our portfolio those which meet our uncompromising standards. With our services, clients streamline business processes, get foundations for sustainable business growth, and cut the cost and duration of innovation adoption.

GlobalDots serves over 350 enterprise customers worldwide, including Lufthansa, Bosch, Fiat, Playtika, AppsFlyer, End Clothing, and more. Our portfolio includes over 80 cutting-edge cloud, web and network vendors, with 12 new vendors introduced in 2020 alone.

We are certified partners of AWS, Akamai Technologies, CloudFlare, Okta, Cato Networks and other world-class players. Our engineers hold CISSP licences from the International Information System Security Certification Consortium.

Trusted By

Takeaway.com AppsFlyer Lufthansa SafeCharge BOSCH Playtika

Austrian Doodle Fyber contentful Perion NI NATIVE INSTRUMENTS

VIDAZOO home24 Guesty ARMIS Rosetta Stone LIDL

GlobalDots

Subscribe BrightTALK Contact Us Schedule a Meeting