

# BNO

GRC Expertise

## How BNO CPA Helped a SaaS Company Achieve SOC 2 Compliance with **DRATA**

[www.bnocpa.com](http://www.bnocpa.com)



GRC Expertise

# How BNO CPA Helped a SaaS Company Achieve SOC 2 Compliance with DRATA

## Client Overview

A fast-growing SaaS provider delivering real-time file synchronization and cloud-based collaboration tools for remote teams recently reached out to BNO CPA to support their journey to SOC 2 compliance. With over 300 corporate clients—including organizations in regulated industries such as finance and healthcare—the company recognized that securing a SOC 2 Type I report was essential to earning client trust and winning larger enterprise contracts.

---

## THE CHALLENGE

While the company had a technically sophisticated internal team and solid security practices, they lacked formal documentation and structure aligned with the SOC 2 Trust Services Criteria. The company selected DRATA as its GRC automation platform, but leadership quickly realized that software alone wouldn't be enough to navigate the intricacies of SOC 2. They needed an experienced audit partner who could provide strategic compliance guidance and deliver an independent, efficient audit process.

That's when the company partnered with **BNO CPA**, a firm specializing in compliance audits using GRC tools like DRATA.

## OUR APPROACH

BNO CPA brought a structured, technology-enabled methodology to the engagement. By integrating seamlessly with DRATA, we helped the company go from initial readiness to a clean SOC 2 Type I report in under 90 days.

**1. ISMS Readiness & Gap Analysis:** We began by conducting a comprehensive gap assessment against the ISO/IEC 27001:2022 requirements. Using DRATA's ISO 27001 module, we:

- Conducting a full control gap analysis against the SOC 2 Security Trust Services Criteria.
- Reviewing DRATA's integrations with the client's systems (e.g., AWS, GitHub, Okta, Jira) to verify proper configuration and evidence collection.
- Delivering a customized remediation roadmap focused on achieving audit readiness efficiently.

**2. Remediation & Control Implementation Support:** Over the next several weeks, we worked closely with the company's internal compliance and engineering teams to implement missing controls and formalize processes. Our work included:

- Advising on the development of essential policies and procedures using DRATA's policy center.
- Ensuring that automated evidence collection was enabled and correctly mapped to all applicable controls.
- Providing walkthroughs and coaching sessions to help internal stakeholders prepare for audit-related interviews and documentation reviews.

This phase significantly accelerated readiness by reducing manual efforts and leveraging DRATA's automation features to their fullest.



**3. Audit Fieldwork:** Once the control environment was stable and operational for a sufficient period, BNO CPA began the formal SOC 2 Type I audit. Using DRATA, we were able to:

- Access most evidence directly through automated integrations, dramatically reducing back-and-forth requests.
- Conduct thorough control testing with minimal disruption to the company's daily operations.
- Maintain open communication with the client via DRATA's platform and regular check-ins to ensure alignment throughout the process.

The audit was completed in under five weeks—well below the typical industry timeline—without any major findings or rework required.

**4. Report Delivery & Next Steps:** We issued a clean SOC 2 Type I report, which the company was able to share with prospective clients and stakeholders as evidence of their security maturity. Our team also:

- Conducting a full control gap analysis against the SOC 2 Security Trust Services Criteria.
- Reviewing DRATA's integrations with the client's systems (e.g., AWS, GitHub, Okta, Jira) to verify proper configuration and evidence collection.
- Delivering a customized remediation roadmap focused on achieving audit readiness efficiently.

### THE RESULTS

SOC 2 Type I achieved  
in <90 days

80%+ audit evidence collected  
automatically through DRATA

No major deficiencies or  
remediation cycles required

Increased stakeholder confidence  
and shortened sales cycles



GRC Expertise

# How BNO CPA Helped a SaaS Company Achieve SOC 2 Compliance with DRATA

## CLIENT FEEDBACK

*"BNO CPA was a game-changer for us. They didn't just perform the audit—they helped us understand the framework, optimize our use of DRATA, and get across the finish line faster than we thought possible. The process was streamlined, professional, and incredibly valuable."*

~ Chief Technology Officer, SaaS Company

## CONCLUSION

This engagement highlights BNO CPA's ability to combine deep audit expertise with GRC automation tools like DRATA to deliver efficient, effective compliance outcomes. For fast-growing SaaS companies looking to meet the increasing demands of enterprise clients, our technology-enabled audit approach offers a faster path to trust and credibility.

## At BNO, We Stand Apart Because we're not Just Another Audit Firm.

**We are the only audit firm exclusively focused on all major GRC (Governance, Risk, and Compliance) platforms, a unique position that allows us to offer specialized expertise and deep insights into the platforms you rely on for your compliance journey.** We partner with industry-leading GRC platforms, ensuring that we deliver tailored services designed for the specific nuances and requirements of each.

Our commitment to focusing exclusively on GRC platforms means we are the go-to experts for organizations navigating the complexities of compliance. Whether you're pursuing SOC 2, ISO 27001, or any other audit, we have the knowledge and the experience to guide you through the process with ease and efficiency. Our team's specialized skill set ensures we understand the ins and outs of each platform's unique functionality and how to best use them for compliance success.