

CASE STUDY

From Providing Security Services to Undergoing a Security Audit

How offensive security company TantoSec achieved ISO/IEC 27001 certification with the help of CyberNinja and Sensiba.

Challenge

Working in the security and compliance space meant TantoSec knew the different frameworks. Couple this with their strong commitment to security, and they knew ISO/IEC 27001 was the framework they needed.

"We obviously pay attention to the processes we put in place. Customers are entrusting us with very sensitive information related to the types of engagements we're doing," said co-founder Marco Cantarella.

Another benefit of ISO/IEC 27001 certification is its use in third-party security assessments and questionnaires. "Getting a standard like ISO/IEC 27001 will help streamline that process," Cantarella said.

From experience, Cantarella and the team knew what was involved in an ISO/IEC 27001 audit. This led them to seek external support from a consulting specialist, CyberNinja. After signing with CyberNinja and beginning to get audit-ready, it was time to bring in Sensiba as the expert audit team.



Overview

TantoSec, an offensive security company, is no stranger to security compliance. They provide cybersecurity services such as penetration testing and red teaming. Founded in 2022 in Australia, TantoSec has grown nationally, and as they are expanding into international markets, they know getting compliant is essential.

Services

- ◆ ISO/IEC 27001

Solution

Initial assessments of TantoSec's audit-readiness showed their policies and documents were housed in different external drives. This static process would make collecting evidence difficult.

With guidance from CyberNinja, TantoSec started using the compliance automation platform Vanta. This took their manual evidence collection and transformed it into an automated process with a clear roadmap. CyberNinja was instrumental in updating TantoSec's procedures to make them compliant with the ISO/IEC 27001 standard. This meant less time creating things from scratch and instead improving what the team already knew. CyberNinja's responsiveness and availability throughout the process made getting audit-ready a lot more straightforward than anticipated.

Once TantoSec was audit-ready, the prep work meant TantoSec's evidence was ready to go in Vanta. This made it seamless for the Sensiba auditors, who are familiar with the platform, to jump in and start testing. Ultimately, this saw TantoSec achieve ISO/IEC 27001 according to their roadmap.



"Overall, it was a very smooth process. Sensiba was available and easy to communicate with. The audit process, in particular, was more achievable than I thought it was going to be"

Marco Cantarella
Co-Founder, TantoSec

Result

With all parties working seamlessly, TantoSec achieved ISO/IEC 27001 certification according to their desired deadline. "Which is a compliment to everyone who worked on it. From CyberNinja to Vanta, and obviously, Sensiba. With all the groundwork we established and the support from those teams it was a really smooth process," Cantarella said.

Whilst achieving compliance is fairly new for TantoSec, they already have their sights set on some of the benefits it's going to bring. "This is going to save us a lot of time and headaches down the road. It's certainly helped move

along some conversations with customers. We obviously expect more things like that to become clearer over time," Cantarella said.

Cantarella also shared his recommendations to other offensive security companies starting the ISO/IEC 27001 process.

"I would recommend Sensiba and CyberNinja. It was easier than I expected it to be. And definitely a lot of benefits to our business moving forward."

"ISO/IEC 27001 is also a worthwhile endeavor. I think that more and more companies are going to mandate something like this as well, just because of the onerous nature of making every single potential vendor fill out a third-party security questionnaire. It just creates so much work. I think obviously it makes our customers' lives easier."

With their sights set on expanding into international markets, TantoSec is already looking into the region-specific compliance standards.

"We want to establish offices in regions like New Zealand and North America. Especially in mature markets, compliance is really important. Overall, we just want to continue to grow the business. The goal is to double in size in the next couple of years," Cantarella said.

About Sensiba

Our risk assurance professionals help you identify, analyze, and manage potential risks. We collaborate with you to enhance the value of your business with customized risk models and experienced support.

Our flexible and pragmatic approach addresses your concerns efficiently and cost-effectively with solutions tailored to your specific needs.