databrackets
cybersecurity • audit • compliance

CASE STUDY

ISO/IEC 27001 CERTIFICATION For Kanini

Kanini Software Solutions wants to be ISO/IEC 27001 certified. But why?

"The customer's perception is reality", as quoted by one of Kanini's leadership team, therefore a Internationally recognized and globally endorsed compliance certification brings credibility and confidence to a client.

Who was the client?

KANINI
Excellence Redefined

Kanini Software Solutions delivers excellence in Custom Software Development.

Kanini Software Solutions anticipated the digital transformation and evolved to be future-ready, dedicating years to build expertise in Cloud Computing, AI & Data Analytics, Product Engineering, Automation, IoT, and Custom Solutions. The journey has led them to be a trailblazer of Digital 2.0, enabling and accelerating digital adoption across multiple industries.

The Problem

Most of the businesses require some standard third-party independent security certification. Lack of security certifications/attestation increases the sales cycle with business prospects going back and forth. Compounding the problem is filling out lengthy security questionnaires.

The lack of a security certification created issues that forced Kanini to take a step back and think through the leading certifications and align with ISO 27001, an international security standard in ISMS. Kanini engaged databrackets to become their certification body for ISO 27001 certification, which will Increase business resilience, align with customer requirement and strengthen customer and partner confidence.

ISO 27001

CASE STUDY

databrackets

cybersecurity • audit • compliance

databrackets's certification process followed a comprehensive, well-structured, systematic two-fold strategy : Stage 1 audit and Stage 2 audit.

The Solution

Identification of Scope:

ISO 27001 Certification audit always starts with the scope description. databrackets helped to define the scope of certification through a detailed study of Kanini's business process and Information Security Management System (ISMS). This was followed by confirmation from Kanini, and both parties entered a contract agreement to seal the engagement and signup for the certification process. In line with the scope definitions, a detailed audit plan was drawn.

databrackets' Assessment and Evaluation platform

databrackets has developed its own compliance Assessment And Evaluation platform that's extensive in coverage, detail-oriented covering all the processes and comes with a fully loaded version of all the controls, complete with a comprehensive dashboard stacked with all the data points for Kanini to get the gist at glance.

The databrackets' Assessment and Evaluation platform made it easier for Kanini to save on time and effort. Kanini was able to submit all the necessary evidence required to meet the audit criteria through this platform at the click of a button. The user-friendly platform equipped Kanini's assurance team to become conversant with the entire audit process.

CASE STUDY
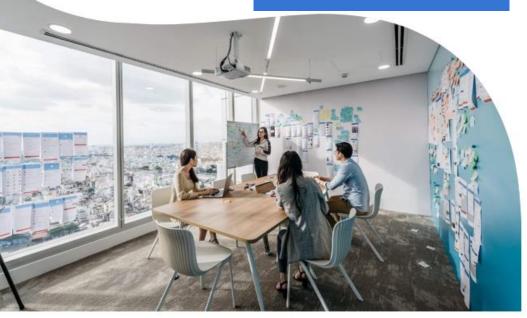
Kanini's team worked with databrackets for about 8* weeks to complete both stage 1 and stage 2 audit requirements.

*Note: The duration will vary for different customers.

The Solution

Stage 1 audit covered all the ISO/IEC 27001 controls prescribed in the standards. databrackets' Assessment and Evaluation platform access was provided to Kanini to do the Stage 1 process's self-assessment. Based on the initial outcome, Kanini submitted relevant documents as proof of adherence. The review process was transparent as all the comments between Kanini and databrackets were recorded. Thereafter, the lead auditor flagged any non-conformance and sought additional information and further clarification, wherever necessary. Stage 1 mainly focused on documentation review. A detailed Stage 1 report highlighting Kanini's ISMS standing was shared, and a call to action was communicated to gear up and get ready for Stage 2.

Stage 2 audit going by the standards stipulates onsite visit at the customer's office, but the pandemic restriction posed a severe threat to physical presence. Hence, the audit was conducted online, which also included a witness audit. A detailed agenda with the opening meeting controls to be audited, the closing meeting was prepared, and the audit set to motion. The pending or partially implemented controls assessed during Stage 1 were closed during Stage 2 by Kanini, who also provided more information on merit.

Once Kanini complied 100% with the stipulated standards, databrackets certified that Kanini's ISMS met the criteria of ISO/IEC 27001.

databrackets
cybersecurity • audit • compliance

CASE STUDY

ISO/IEC Certification reduced the conversion time in a customer vetting Kanini's profile by 50%.

Result

1. The ISO 27001 certification is a market differentiator as its acceptance and adoption rate is on the rise in the United States and gaining recognition on a global scale.

2. Organizations prefer to deal with service providers holding reliable risk-based ISMS certificates specific to the information security

3. Achieving ISO 27001 certification is an authentication that Kanini has been. independently assessed to an international standard based on industry best practices

4. Certified to an international standard will most certainly impact Kanini's bottom-line positively as it positions to endless possibilities.

5. The ISO 27001 Certificate has a good potential for Kanini to grab opportunities and sign deals with companies where security is a critical element, who favor someone with certified security management.

Case in Point

Interestingly Kanini recalled an instance when a customer asked to fill 350 questions to vet their profile unless they have a third-party certification like ISO 27001 or SOC 2. Filling 350 questions would have taken a minimum of 4 to 6 weeks. Kanini could have saved time and effort by just submitting the ISO 27001 certificate instead of the hassle of filling the questionnaire. The prospect would have signed the agreement based on the certificate as proof of Kanini's compliance and competence in security standards and measures.