Streamlining ISO 27001 With a Virtual Audit

Lucidworks turned to Sensiba and Drata for a smoother, more efficient recertification

Challenge

Following a less than ideal situation with an ISO 27001 auditor that relied on manual processes and communication, AI-powered search and product discovery software provider Lucidworks turned to Sensiba for a smoother, more efficient audit to provide its ISO 27001 recertification.

Lesley Heizman, Manager of Risk & Compliance, says Lucidworks' previous audit firm didn't offer a modern virtual audit option, instead relying on voice calls and swapping audit files via email. The firm did not communicate outside of the audit, and the Lucidworks team didn't feel comfortable asking questions about the process.

Overall, the firm was a poor cultural fit with a vibrant Bay Area tech startup like Lucidworks.

> "Working with a company of a similar size and that offered startup experience was important to us. We were comfortable the Sensiba team was open to our questions, and they were very responsive."
>
> **Lesley Heizman**
> *Manager of Risk & Compliance, Lucidworks*

"The process was so painful," Heizman says. "We'd spend hours on the phone each day and we were emailing files back and forth. We wanted someone who was more modern in their approach."

Lucidworks

Overview and Services

Lucidworks powers the search and discovery experience for the world's largest and most successful companies. Lucidworks' solutions personalize the search and discovery experience to reveal actionable insights about user intent and rapidly deliver them to the relevant channels of engagement. Customers rely on Lucidworks' products to power commerce, customer service, and workplace applications that delight customers and empower employees.

◆ ISO 27001 Recertification Audit

◆ SOC 2 Type II Audit

Solution

To streamline the audit process, Lucidworks implemented the Drata GRC compliance platform to map its controls and automate audit documentation. Drata, in turn, recommended four potential audit firms and Sensiba quickly stood out.

"Working with a company of a similar size and that offered startup experience was important to us," Heizman says. "We were comfortable the Sensiba team was open to our questions, and they were very responsive."

Lucidworks also appreciated Sensiba's virtual audit methodology. For instance, the Sensiba and Lucidworks teams leveraged the Drata platform to exchange documents throughout the process.

"There was a lot of information that could be shared directly within Drata, which saved hours of time on our part," Heizman says. "And our conversations were much more productive because everyone had the materials they needed and we could dive right in."

Sensiba's audit approach included a virtual walkthrough of Lucidworks' location in San Francisco's Financial District, saving time and costs.

Result

Achieving ISO 27001 recertification provides important validation of Lucidworks' information security controls and processes.

"We have customers in the engineering and manufacturing sector, the financial space, and outside the United States," Heizman says. "They expect to see compliance with a variety of quality management and security frameworks, but ISO 27001 is especially important."

The Drata platform enabled Lucidworks to streamline other security-related audits, such as SOC 2 Type II (also conducted by Sensiba). Lucidworks was able to leverage SOC 2 evidence to provide a headstart on its ISO 27001 recertification audit.

"Doing the ISO audit gave us a strong starting point from which we could branch out," Heizman says. "And now we're seeing concerns about privacy and AI, and other components that are available within ISO."

Heizman recommends companies exploring the ISO 27001 audit process look for audit firms that can provide a collaborative relationship. While the auditors have to maintain their independence and won't provide prescriptive advice, they can help clients understand the process and discuss accepted practices in general terms.

"I'd say to anyone that even if you feel you're not ready, it's never too early to engage someone," she says. "The only way you can get a true feeling where you stand is talking with your auditors and figuring out if you need to shore up processes or controls."

> "Even if you feel you're not ready, it's never too early to engage someone. The only way you can get a true feeling where you stand is talking with your auditors and figuring out if you need to shore up processes or controls."
>
> Lesley Heizman
> *Manager of Risk & Compliance, Lucidworks*

About Sensiba

As a certification body, Sensiba conducts audits against a variety of standards including ISO 27001, ISO 27017, ISO 27018, ISO 27701, ISO 42001, SOC, HIPAA, NIST, and others. ISO 27001 provides a cost-effective cybersecurity framework to help organizations, including those delivering solutions on the cloud, understand their security risks.

ISO 27701 is a privacy extension to ISO 27001 that maps closely with GDPR. ISO 42001 is a new standard related to Artificial Intelligence to ensure companies that use, develop, or produce AI tools, are managed properly.

These certifications can be valuable in highlighting an organization's commitment to managing information security and privacy.

Contact us to learn how our cost-effective audit methodology can benefit your organization.

Brian Beal   e. BBeal@sensiba.com
Partner, A&A   p. 925-271-8556