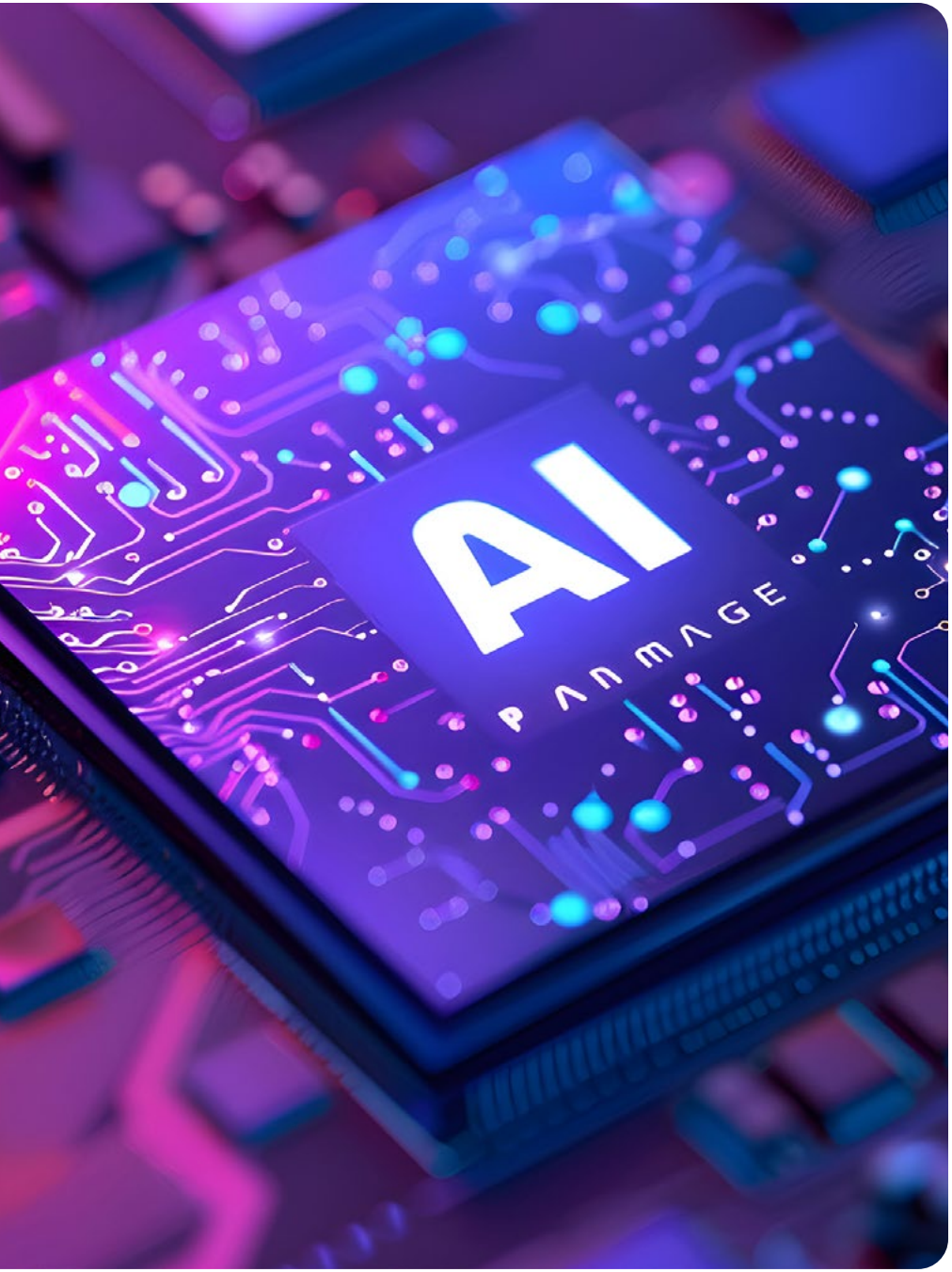
schellman
Quality. above all.

STACKAWARE PIONEERS RESPONSIBLE AI BY BECOMING ISO 42001 CERTIFIED WITH SCHELLMAN

StackAware

In StackAware's effort to practice what they preach as leaders in AI governance and security, they partnered with Schellman early on to achieve ISO 42001 certification.



As a global leader in cybersecurity assessments, Schellman specializes in services like ISO, FedRAMP, SOC, and PCI. To continue to meet the ever-evolving needs of clients amidst the ongoing adoption of AI across industries, Schellman has expanded their ISO services by becoming the first ANAB accredited Certification Body for ISO 42001.

Similarly, in StackAware's effort to practice what they preach as leaders in AI governance and security, they partnered with Schellman early on to achieve ISO 42001 certification. In doing so, StackAware continues to lead the way in fostering and providing responsible AI development and usage throughout their practice and is now prepared to help other companies become ISO 42001-ready too.

STACKAWARE AND SCHELLMAN'S STRATEGIC PARTNERSHIP

StackAware helps companies measure and manage their AI risk to maintain security, privacy, and compliance. Their AI governance expertise, combined with the need to stay abreast of the transforming compliance and technology landscape, made it an obvious choice for StackAware to pursue ISO 42001 certification. And partnering with Schellman, an indisputable trailblazer in the space, was another easy decision.

"I really learned about ISO 42001 toward the end of 2023," explains Walter Haydock, Founder and CEO of StackAware. "Since StackAware is in the AI governance space, I thought it's something that I should be familiar with and understand. And the more I looked into it, the more I realized that it would be a big opportunity for my company from a business perspective. And at the same time, I would need partners who could conduct these audits."

From an audit and compliance perspective, StackAware had not previously gone through the process with an independent assessor, having regularly taken more of a customer due diligence approach. Haydock explains that Stackaware "might be an internal auditor, but [we are] certainly not a certification-granting external auditor," so he knew they needed to find a trustworthy partner in their pursuit of ISO 42001 certification.

When searching for such a partner, Schellman stood out as a leading provider of attestation and compliance services in the AI governance space and as the first ANAB accredited Certification Body for ISO 42001. "So, what I did was scan the market to look at all the firms out there who were potentially going to be offering it. And I saw Avani Desai, your CEO, do a webinar on 42001, I actually direct messaged her on LinkedIn and she got right back to me. That's how we got moving." Haydock goes on to credit Schellman as being proactive, quick, and willing to work flexibly as the main drivers in choosing the firm as his trusted partner.

ACHIEVING ISO 42001 CERTIFICATION SUCCESS WITH SCHELLMAN

With the ISO 42001 standards being so brand new in the market, StackAware had a bit of a natural learning curve at the outset of the audit. To tackle this, they invested in a gap assessment—something Haydock highly recommends, as it helps when becoming familiar with the framework's requirements. "I would recommend doing that gap assessment first because that highlighted a lot of things to me that were important for the audit."

For instance, in their work, StackAware tries to make everything machine readable and reusable using structured databases and functions to reduce variability and manual effort. "The issue is that it's very challenging to present that to someone who isn't intimately involved in the inner workings of our system. So, making sure that there was an easy way to create human readable documents from our underlying data was important."

That need to export this information in a more presentable way was discovered during StackAware's readiness review and in response, Schellman worked with StackAware to get to a point where all their policies and procedures became trackable in a structured database. Now, an auditor can more easily interrogate the information and make sure the necessary requirements are being met and simultaneously, StackAware knows they are keeping a single source of truth without risk of duplicative entries.

When the more in-depth certification audit commenced, Schellman adopted a customized approach to work flexibly with StackAware, including meeting their business standards when dealing with sensitive and confidential information. Haydock explains that "building the AI management system documentation with the view for external review" was an important step, and that Schellman helped in establishing "a structured set of Google Drive folders that [StackAware] could control the permissions to." In the end, Schellman had "access to the confidential information for StackAware and at the same time, I could have something that's public facing that didn't have that sensitive data."

Finding this balance was a crucial component of their effective partnership and successful audit. “[Haydock] is a firm believer in transparency” confirms Zuby Alikhan, Senior Associate at Schellman who lead the ISO 42001 certification review for StackAware. He explains access to this publicly available information “made it relatively easy to ask the questions we need to and even ask more in detail to understand [StackAware’s] perspective on how [they] meet they addressed AI risks and met their overall objectives.”

Alikhan stresses the importance of adopting this kind of cohesive collaboration when tackling ISO 42001 certification, “it was a mutual understanding the standard is new for both of us, and the belief of transparency and openness made the auditing process smooth.” Haydock agrees that this synergy led to a powerful partnership, “we worked together to come up with a flexible way to get the audit done while at the same time meeting our business objectives.”

StackAware's extensive preparation and willingness to be transparent were invaluable, and Schellman's proactive communication also contributed to their effective partnership. "[Haydock] is a firm believer in keeping meetings as efficient and concise as possible" explains Alikhan, so Schellman made sure to always come prepared. He shares Haydock "prepared evidence in advance within Google Drive and asked us to review it" ahead of meetings.

For example, "a week prior to stage 2 fieldwork, we received an e-mail asking for us to review" the compiled evidence and proactively, Alikhan "started asking questions using the comments functionality" so that Haydock was able to respond accordingly. Alikhan explains, "this continued leading up to the official week of fieldwork", although he strategically saved "the questions that are better suited for a demonstration or that required more back and forth" for their meetings. Schellman's proactive approach and thorough preparation proved to be an efficient strategy when dealing with the complex topics that arise throughout the assessment.

> It was a mutual understanding the standard is new for both of us, and the belief of transparency and openness made the auditing process smooth.

ZUBY ALIKHAN
Senior Associate
Schellman

Schellman's expertise and tailored approach also aided StackAware in figuring out how to structure a risk register, especially considering "there weren't really any kind of certified AI impact assessments" already in place, Haydock explains. He appreciated working with Schellman to "come up with an effective way to present that information that captured all the relevant risks for the assessment and the impact assessments, which are unique to 42001." Combining both StackAware and Schellman's perspectives in addressing the new standard, paired with mutual openness, collaboration, and transparency allowed for an effective audit experience.

LEARNED ESSENTIALS FOR 42001 CERTIFICATION EXCELLENCE

In fact, the combination of both parties' proactive preparation and Schellman's thoroughness as assessors were critical to the StackAware's eventual successful ISO 42001 certification. "As the founder, I was very focused on getting this done. This was not a secondary priority. This is a primary effort for the company," says Haydock. He goes on to advise that other companies should adopt a similar approach, though they should be ready for the work involved. "For companies that maybe aren't AI governance

companies, this is not something that is a casual effort. And it's challenging because there are potentially auditors out there who might take a kind of a lighter touch approach or might take a more rubber stamp approach, and Schellman is certainly not one of them."

Haydock specifically calls out the need to dedicate the appropriate level of attention and management focus towards this effort, "especially if you're doing this for the first time, which is true for most people, you're really going to need to do a lot of preparation to and allocate the resources to make sure that it's done correctly. And it's going to be a learning experience for everyone."

As part of that preparation, Haydock explains "you probably want an internal auditor who is not part of the organization because that person is going to be more willing to point out things that might seem normal to you but might not seem normal to a contractor."

"For companies that maybe aren't AI governance companies, this is not something that is a casual effort. And it's challenging because there are potentially auditors out there who might take a kind of a lighter touch approach or might take a more rubber stamp approach, and Schellman is certainly not one of them.

WALTER HAYDOCK
Founder & CEO
StackAware

He takes this advice a step further, explaining that because an internal auditor won't know your business as well as you do, "coming up with an effective way to have the dialogue to document all of the findings, and then respond to them" is important. Additionally, Haydock suggests planning ahead, "I wouldn't try to jam in the internal audit the last second right before your external audit," because that would lead to unnecessary and avoidable challenges.

Equally as important as thorough preparation, Haydock recommends adopting a forward-thinking mindset post-certification, because "it's not a one-and-done process" so once you're certified, your 42001 journey doesn't end there. "For example, we're going through a risk and impact assessment for Google Workspace features because Google's adding some additional tools right now, and that's something that we need to continually do as part of the 42001 process."

It's similarly important to understand that this process will require continual attention and regular updates as your practices and procedures evolve over time. Haydock adds, "make sure you have the resources allocated for continuous adherence to the standard."

And then, when undergoing a certification audit, Haydock emphasizes the importance of securing the right partnership that is tailored to your business needs. "As far as the auditors go, having an organization that can work to pull the data or view the data in a way that works for you is important." Because there isn't a universal tool or standard format already established, it's important to find an auditor, like Schellman, who can be flexible and work with you to get the necessary information in a way to makes sense for both parties involved.

Moreover, Haydock stresses the importance of finding an auditor with whom you can have honest and collaborative conversations. "You want to have a collaborative relationship with the auditor, not hide things from them." Haydock explains he felt comfortable surfacing nonconformities and how he addressed them with Schellman, and he trusted Schellman to disclose whether StackAware met the requirements effectively or not.

In agreeance, Alikhan confirms “one of the biggest takeaways is just having an open line of communication and an open train of thought.” He continues, “we may see one thing a particular way as auditors, but then a client may see something their way” at the same time. “So, it's always important to see how they align themselves with the standard and how we can assess that with conformance and go from there.”

Alikhan goes on to praise Haydock for being receptive to addressing findings that were discovered throughout the process, “throughout each review, [Haydock] actioned upon the findings received and was open to feedback with reasonable explanation.” With the ISO 42001 certification process being as new and dynamic as it is, a direct, receptive, and collaborative partnership is essential for certification success.

> One of the biggest takeaways is just having an open line of communication and an open train of thought. We may see one thing a particular way as auditors, but then a client may see something their way. So, it's always important to see how they align themselves with the standard and how we can assess that with conformance and go from there.

ZUBY ALIKHAN
Senior Associate
Schellman

THE PERKS OF BEING AN ISO 42001 CERTIFICATION TRAILBLAZER

All the work performed to prepare and in finding the right auditor proved well worth it, as the benefits of becoming ISO 42001 certified include proof of organizational dedication to secure and responsible AI management and development. This leads to enhanced trust with stakeholders, improved risk management, and an undeniable competitive advantage—something Haydock can attest to firsthand.

For Haydock, StackAware becoming 42001 certified has "certainly been a business driver" as they continue to acquire more customers to work with for 42001 readiness. So much so that StackAware is hiring employees so they can help even more customers become ISO 42001 ready. That said, Haydock acknowledges the competition is fierce as more companies continue to follow their lead and join the fray.

Nonetheless, ISO 42001 certification remains a significant business growth opportunity, and being certified early has certainly helped StackAware stand out due to the clear downstream impact on value and credibility. Still, the biggest value-add from ISO 42001certification is the third-party validation of an organization's trustworthy AI systems and their related responsible management practices.

Haydock explains there is a "lack of information or lack of guidance on responsible AI" and as a result, "there is a lot of variability in what companies are doing in terms of AI." With so many companies releasing generic high-level responsible-AI statements that lack transparency, or failing to even disclose the type of AI models they use, it's hard to know what their AI governance structure looks like. Moreover, it's nearly impossible to know how or if they are actually being responsible with their AI use.

But in getting the established ISO 42001 standards in place and becoming certified, organizations can "prove that you have an effective AI governance program and meet the mandatory requirements," which will aid in building trust and scaling AI systems into the future.

> An AI management system gives you a framework to comply with any regulation or requirement...we're ingesting these business requirements, legal requirements, ethical requirements. We're analyzing them, and then we're looking at the risks. We're looking at the systems we're using, and then we're applying these controls.

WALTER HAYDOCK
Founder & CEO
StackAware

THE FUTURE OF ISO 42001 AND EVOLVING REGULATIONS

When reflecting further on the value of ISO 42001 amongst evolving regulations, Haydock explains, “an AI management system gives you a framework to comply with any regulation or requirement.” In other words, it gives you a structured process for saying, “we're ingesting these business requirements, legal requirements, ethical requirements. We're analyzing them, and then we're looking at the risks. We're looking at the systems we're using, and then we're applying these controls.”

Secondly, “there are specific statutes that name ISO 42001.” For example, these types of regulations and standards are going to be very important in the EU. “On top of the EU AI Act, you have things like the product liability directive, which is being revamped, and the AI liability directive, which may be a separate requirement. So, figuring out how companies are going to comply with these regulations is very important if they want to do business in the EU,” and ISO 42001 certification can provide an excellent foundation.

Haydock did go on to acknowledge that there has been some confusion around the future of 42001, or more so “the interplay with the EU AI Act, because the joint technical committee released a report in 2023 that pointed out some gaps in 42001.” With that being said, “the committee leader said he's not going to be able to release the harmonized standards, which give you a presumption of conformity under the regulation, until the end of this year [2025]. And I don't see a new standard being created by the end of this year.”

So, while ISO 42001 isn’t going anywhere any time soon, it’ll likely expand and evolve just like any other certification in the compliance and technology landscape. “What I predict is that there's going to be 42001+ some specific Annex A controls that will be required. It'll be 42001+ that will become a harmonized standard under the EU AI act.”

Regardless of what's to come, StackAware can proceed with confidence that they are moving into the future of AI responsibly and ahead of the curve thanks to the collaborative guidance of Schellman in their successful pursuit of ISO 42001 certification.

schellman

Quality, above all.

schellman.com

4010 W Boy Scout Blvd / Suite 600 / Tampa, FL 33607

1.866.254.0000

Outside of the United States, please dial: +1.813.288.8833

Follow @Schellman on Social Media:

Certified B Corporation