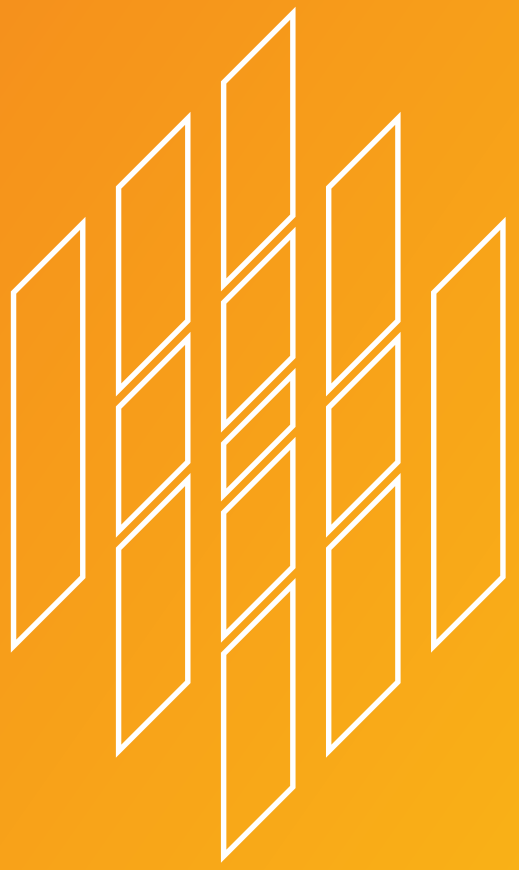
schellman
Quality, above all.

# ZS Associates Establishes Common Control Framework to Achieve Compliance Efficiency

ZS



When their business began to expand, ZS Associates realized they needed to find the perfect medium between compliance and efficiency in order to maintain their customers' trust. They found it in an internal implementation of a common control framework—an effort that has since helped them streamline their current compliance endeavors while also positioning them well for their bright future.

As more compliance standards and programs continue to emerge, organizations across the global business landscape face more decisions on which certifications and examinations suit their needs the best. The compliance facet to any business has always represented a challenging endeavor, and it's no secret that finding efficiencies amongst the seemingly endless preparation and planning of audits makes for a desired advantage.

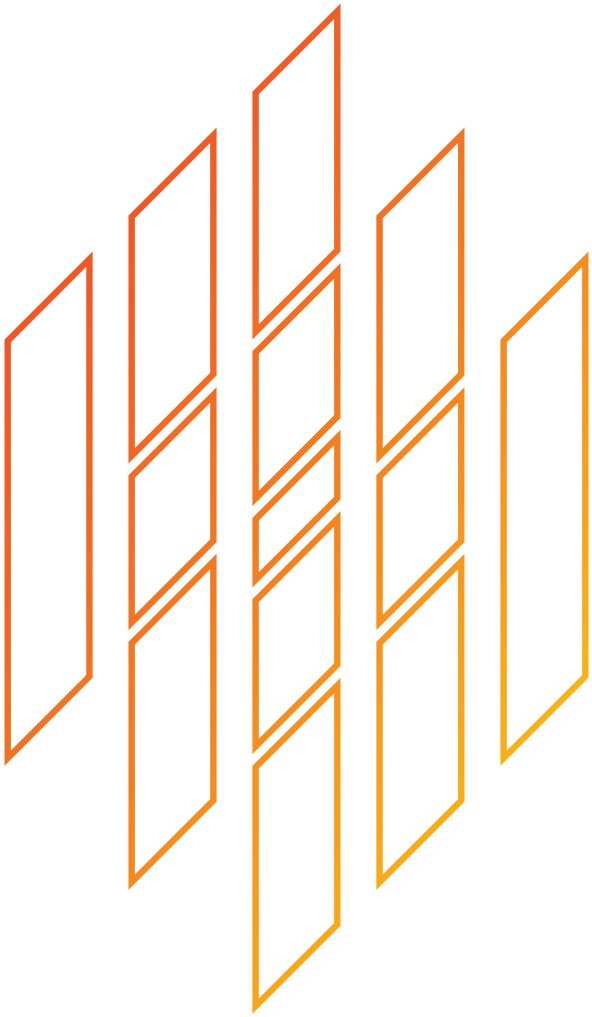
For ZS Associates (ZS), this desired advantage became a priority—a dubious undertaking at first that paid off after the diligent work of their personnel in conjunction with advice from their chosen auditors at Schellman.

Founded back in the 1980s, ZS began with two employees, and has grown into a successful business of over 10,000 staff today. A professional consulting firm, their primary focus began within the pharmaceutical industry and has since expanded to include health plans, financial services, technology services, and travel and hospitality as well. As their industry reach continues to broaden even today, so have their compliance needs, prompting an ambitious internal initiative that they hoped would help streamline all the efforts they would need now and in the future.

# Efficiency and Flexibility as a Goal

The initiative? To create a common control framework for multiple services.

"It's obviously a great idea in theory—to create something you can leverage for more than one need. But in reality, this is something that a lot of organizations struggle with," says Rob Tylka, Principal at Schellman and leader of their Midwest practice. "In the case of ZS, they have obviously been more successful in this regard. When you consider how many clients they have and the varying services they provide—the compliance complexities all that adds—it really is quite remarkable."



Despite the enormity of the undertaking and the uphill battle they faced, the idea—when those at ZS realized it—stuck. They were determined to establish a common control framework to marry their compliance initiatives and efficiency. “We wanted to ensure that while we meet the complexities of each compliance requirement, at the same time, it must be easy for our teams to adopt and adapt,” explains Ali Khan, IT Governance, Risk & Compliance Manager at ZS. “But not only that, we always keep a watchful eye on what could potentially work not only in the present but also in the long run — we are already moving towards a new approach where our clients can easily leverage our applications, products, algorithms and data through our easy-to-adopt platform ZAIDYN.”

We wanted to ensure that while we meet the complexities of each compliance requirement, at the same time, it must be easy for our teams to adopt and adapt.

– Ali Khan

***ZS*** | *IT Governance, Risk & Compliance Manager*

# Compliance as a Priority

Compliance has been a strong priority for ZS since the start, as evidenced by their well-structured team dedicated to it that features both formal and informal committees in place, bound together and focused on security. “This is taken very seriously by all of us,” reiterates Khan. “We know it only takes something small to cause a big problem. For us, awareness more of a ‘must-have’ than a ‘good to have.’” This push for awareness represents an important part of ZS’s established control framework.

When an organization grows at the rate ZS has and still is, onboarding new personnel remains a key component in maintaining their established culture of compliance. “We recognize that the way you approach an organization with a few thousand people is different than the way you approach a firm with 10,000 people and growing. And so, we continue to identify additional points where we can reach out and talk about information security. When new hires are onboarded, a specific portion of their orientation program focuses on privacy and security. We also simulate monthly phishing campaigns firmwide and update our privacy and security training every year to continue to make that engaging,” explains Christine Milkowski, Senior Legal Counsel and Data Protection Lead for ZS.

But it’s not just a stringent awareness among their people—ZS has taken care to invest in technology as well. “We also believe in a lot of preventive controls rather than adopting detective and administrative rules. Annually, we focus heavily on technologies that fill gaps and help our people apply best practices. It’s all about helping ZSers succeed,” says Khan.

# Finding the Base

When it came time to evaluate all these controls put in place, ZS contracted with Schellman for audit work, and the initial agreement was for a singular SOC 1 examination of their Javelin platform. But with the rise of SOC 2 as a popular standard within the marketplace, the organization soon followed the trend and added the service that would eventually provide the basis for their common control framework.

“That was a pretty easy decision for us. We’d always done well with the SOC 1 report, but then when the SOC 2 became available, and we reviewed the objectives in there and the applicable controls, we really thought it enhanced what we were already doing,” says Milkowski. “Going to the SOC 2 was easy because we've always been really focused on security, compliance, and confidentiality - being able to hold a stronger assessment out to our client was a no-brainer.”

From there, client demand meant adding more and more to the ZS compliance portfolio, including ISO 27001. At that point, the firm pressed pause—an ISO certification was a significant undertaking. “We deliberated internally among leadership, and what ultimately helped us with our decision was asking the right questions. Why do we want to do this? And why would we bring in an ISMS just for one client?” states Khan. Together, they realized, “why not for our entire organization?”

Going to the SOC 2 was easy because we've always been really focused on security, compliance, and confidentiality - being able to hold a stronger assessment out to our client was a no-brainer.

– Christine Milkowski

***ZS*** | *Senior Legal Counsel and Data Protection Lead*


# Scalability Across Complexities

With the idea now to implement a common control framework, those at ZS got to work. The idea was to create something that would be audit-ready—"something we could prepare once and leverage," says Khan. But that idea wasn't without its hurdles. "We wanted to ensure that our entire service delivery model was being secured across the board. So, be it a consulting project, be it a technology project, are we able to have some level of security delivered to our client? Because at the end of the day, good quality and a good compliance solution are tied to strong customer satisfaction."

Though the new priority was the ISMS for their ISO 27001 obligation, ZS's previous SOC 2 for their Javelin platform paved the way for some control overlap. "We had to enhance our policies and procedures, apply more reporting metrics, and sort our documentation. That's where we added in some flavor to our common control framework related to ISO," explains Khan

Having provided several services and participated in scoping discussions for various compliance initiatives at ZS, Schellman personnel were impressed with their client's dedication. "From what we've seen in the marketplace, everybody wants to put together a common control framework. It's a big need, but we find it oftentimes hard for organizations to implement, because usually, controls are not a one-size-fits-all approach and must allow for some kind of flexibility, depending on the type of service," explains Tylka. "But ZS has found that baseline of commonalities, and what they have in place now really sets them apart from their competitors."

From what we've seen in the marketplace, everybody wants to put together a common control framework. It's a big need, but we find it oftentimes hard for organizations to implement, because usually, controls are not a one-size-fits-all approach and must allow for some kind of flexibility, depending on the type of service.

– Rob Tylka

***Schellman*** | *Principal*

# Using the Right Resources

Though some of the labor-intensive implementation of their framework was done internally, predating the relationship with their auditors, those at ZS still credit the assessors as having been a help. “Having Schellman as a trusted partner helped us dive in more. They’re absolutely an asset,” says Khan.

“Compliance is often seen as a fear-driven concept in the workplace—people are scared of it. But one of the biggest things about Schellman is amplifying the simplicity behind it,” continues Khan. “Rob and his team have always made it very easy. Some roadblocks seem like rocket science to us, but you take it to them and they say, ‘that’s a good question, let me solve this for you.’ This simplicity and reliability built the trust we have now.”

Both firms expect their partnership to continue and grow as the consultants look toward the future and continue to adapt their established framework. “Even when we come across situations today, it’s great to know that we have somebody we can immediately reach out to. We know that we will get the support to help us move ahead and navigate further. Schellman is our go-to when we talk about compliance and audit. We’ve been trying hard to keep expanding our relationship,” confirms Khan.

Compliance is often seen as a fear-driven concept in the workplace—people are scared of it. But one of the biggest things about Schellman is amplifying the simplicity behind it.

– Ali Khan

***ZS*** | *IT Governance, Risk & Compliance Manager*

# Necessary Additions Made Easier

And that necessary adaptation certainly will come—it already has, in some cases, having been prompted through global regulatory requirement changes and ZS's expanding market space. "A year ago, we didn't have a local presence in terms of applications and products in China. We've got it now," says Khan. With that came new requirements to meet. "And one of the pieces that helped us achieve this was that we didn't have to start from scratch. A lot of controls that Schellman helped us mature in our other software programs formed the foundation that we built upon." Aside from Chinese expansion, ZS continues to add different kinds of services, and with the regulations that come along with that, the firm understands that they will need to remain vigilant and flexible.

Not only that, but they'll also need to ensure they go beyond the legal requirements to satisfy what's arguably just as important—their customer obligations. "In addition to all these regulatory changes that we are monitoring and reacting to, we are also monitoring how our clients are reacting to them," offers Milkowski. "For example, GDPR has been around for a few years, and it allows the flow of personal data outside the EU if certain conditions are met. However, we have some clients who may prefer local EU hosting. So, as a global consulting firm, we are monitoring our client expectations on top of all these regulatory changes."

# Looking to the Future

Despite the anticipated modifications that will become necessary—some known, some unknown—ZS feels confident that their established control framework will continue to serve them well in providing them more efficiency during their compliance audits.

"The common control framework that we've set up is intended to be flexible and scalable. We have all of these objectives that we're meeting globally in all of our offices, in all of the different countries where we have operations. And when there's been a change in our compliance obligations we've been reactive to that change—or in certain cases, we're monitoring and anticipating it, which is the best-case scenario. Whichever it is, we're able to modify our controls and change what we're doing at a local level without affecting our overall framework," says Milkowski.

For the firm, the ability to make those minor tweaks—as opposed to larger security changes—has been well worth the arduous framework implementation process. In fact, there's not much ZS thinks they would have done differently, knowing what they know now after their success.

Though there is one thing: "I would've gotten the ISO certification earlier," admits Milkowski, and others involved in the process also believe that, as a starting point for such a lasting, all-encompassing endeavor, ISO 27001 makes a lot of sense. "Absolutely. ISO as a base would have made a lot of changes easier because that would have covered a lot of ground," agrees Khan. But even still, "it's been a natural progression. We have had moments, wonderful learnings that came with the way we did things. I think that's the beauty of it, right?"

# A Long-Term Solution

In fact, if there are other organizations across marketplaces with an urge to implement a similar framework, there is one core facet that ZS believes must be the foundation—more than a SOC 2 base, more than the addition of ISO 27001. To be successful in creating a common controls framework, it is essential to begin with a strong, fully permeated attitude toward security and compliance.

“You have to treat these things as second nature—not because somebody’s asked you to do it. We do it because it’s the right thing,” emphasizes Khan. “We embody a ‘do it right’ attitude not just at the top but at a grassroots level as well. That’s what makes these types of decisions easy to make and implement.”

ZS has proven that establishing a common control framework is, in fact, possible. “Having served as ZS’s auditor for the past decade, it is remarkable how robust their control framework is given the unique demands of the industries they serve and services provided,” adds Tylka. “It is something to be envious of.” As ZS continues to look forward, working through expansion and various changes to their business portfolio, that attitude towards security and compliance will remain steady and strong. With the common controls framework functioning efficiently, the path towards progress appears smooth.

As we reflect on ourselves now, there's always room for more—we're already planning our next step forward. We'll continue to focus on automation in control management, testing, and accessions in the industry. As it always has, this framework will continue to deliver value and a solid foundation for years to come.

– Ali Khan

***ZS*** | *IT Governance, Risk & Compliance Manager*

schellman
Quality, above all.

www.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

ZS ASSOCIATES ESTABLISHES COMMON CONTROL FRAMEWORK