# SecureFrame

by Head of Product

Compliance Infrastructure | Compliance Certification

## Details

| | |
|---|---|
| Review Date | 07/31/2023 |
| Purchase Date | N/A |
| Implementation Time | N/A |
| Product Still in Use | Yes |
| Purchase Amount | N/A |
| Intent to Renew | N/A |
| Review Source | Elion |

## Product Rating

| | |
|---|---|
| Product Overall | 5.0 |
| Use Case Fit | 5.0 |
| Ease of Use | 4.5 |
| API | 5.0 |
| Integrations | 5.0 |
| Support | 5.0 |
| Value | 5.0 |

## About the Reviewer

Purchasing Team | Implementation Team | Product Oversight

## Reviewer Organization

N/A

## Reviewer Tech Stack

N/A

## Other Products Considered

Drata | Vanta

## Summary

- **Product Usage: SecureFrame is used by the organization to manage secure information and ensure compliance with regulations such as SOC 2 and HIPAA.**
- **Strengths: SecureFrame delivers on its promise of providing a less painful audit process, offers good support, and uses a mix of expertise from technical to legal to business operations.**
- **Weaknesses: The audit list provided by SecureFrame can feel overwhelming and could be better prioritized.**
- **Overall Judgment: SecureFrame is confirmed as the right choice, delivering value for its cost and likely to be used for any future SOC 2 Type II certification.**

**Today we're talking about SecureFrame and how it's used at your company. Could you give us a brief overview of the company and your role there?**

I'm the Head of Product at a company that's building a tool that makes it easier for consumers to make healthcare decisions, with a focus on what you can afford. So, we're building a financial decision-making tool in healthcare. When you go to select your insurance plan at open enrollment, we take your previous claims data from your employer or previous insurer, and run those claims against every possible plan option you have. That allows us to give you a pretty precise number as to what it will cost you to be on plan one, two, three, or four. This helps save the employee money by picking the right plan that meets their needs and passes big savings to the employer who's paying the brunt of the premium bills. We would not consider ourselves a care navigator or a front door for health. We're really trying to figure out how patients can pay for the things that they need in an affordable manner.

**Why did you need a product like SecureFrame's? What were you evaluating when you looked into working with them?**

As a primarily B2B healthcare business, you are managing a certain amount of secure information. You have to abide by regulations that are quite strict. We comply with HIPAA, which is the most common compliance requirement for companies like us. Beyond HIPAA, you have a number of other requirements, like SOC 2.

Most companies have to figure out how to get these certifications. In the old days, that meant talking to a consultant, who would come in to review everything one has, from documentation to our infrastructure to our data management practices. They would talk to our employees, look at what software is on the computer, and then essentially spit out a checklist of thousands of things one had to do as a corporation to get certified. If you fulfill 90% of those things, it's likely that you will pass an audit and get a certification – that's how SOC 2 works.

You need these certifications to be able to sell in the healthcare industry. That's goal number one and why most companies do this. The second is that it is actually a good way of practicing and making sure that you're abiding by the laws and protecting users' and business information appropriately. This allows us to continuously build trust with our users and buyers.

With companies like SecureFrame and Vanta – you could call them tech-enabled auditors – they use APIs and connections to different pieces of software, given that everything is on your computer in the cloud, to run the audits. They automate the vast majority of things that those on-hand consultants would have done and then automatically produce that checklist for you. And in certain circumstances, they can go in and automatically run fixes as well. I'd say that last piece is minimal. The hard part is to identify where you're off and to have a good prioritized list of the most important things to finish first: things that you absolutely will not pass your audit if you don't complete.

The other thing that's really important is that these tools are continuously running. SecureFrame is constantly rechecking your system and making sure that you're still in compliance. So, oftentimes, this goes into flux when you have new hires or off-boardings. Introducing new individuals to your secure data creates the biggest risk. For example, we brought in someone new two months ago, and our SecureFrame rating dropped 20 points because there was someone who hadn't taken trainings or done eight other required things. We would not have passed an audit if we had been audited at that moment. So, a tool like SecureFrame gives you a lot of peace of mind. It gives you a lot more protection when you're going in. Ultimately, it considerably lowers the cost of going through the entire audit and certification process by at least a third, if not more.

**What is the cost of going through one of these audits? Does that include both a monetary and a time cost?**

Both. The time cost is more expensive than the monetary cost. You end up using a lot of different resources to put together a lot of different documentation. I remember when we went through this at a previous company, it was easily like a million dollar project. At another large organization I used to work at, we ended up spending around $200K just on the audit, not even on the steps to get towards the certification. In that situation, we had to do it twice because of how massively we changed the system between checks. It's usually single contracted SOWs (statements of work) of $50K+ to run an audit. You then have addendums or additional SOWs to do the actual certification process. If you want the contractor to do any of the actual implementation of the changes or the policy writing, that is its own statement of work. All of these pieces stack up and end up becoming quite expensive.

I don't remember what Vanta's exact pricing is, but when we looked at them at a previous company, they cost about 1/3rd to 1/4th of the external auditors we were evaluating. The only reason we didn't go with a software solution at the time was that, being a large public company, our legal team was very uncomfortable without having senior legal counsel on the auditors' end. That risk felt too high to them at the time, so they wanted to get professionals that understood our unique system and had their own legal side to discuss issues with.

**So, organizations like SecureFrame prepare you for the audits by giving you the software and the checklists and actually run the audits.**

Yes, they run everything. If you do the full checkup, it gives you a score pretty much instantaneously, and it's ongoing. And then you go and implement the changes and policy updates to ensure you're still in compliance, but they're going to do the vast majority of it. Most of their side is done automatically through their technology. They do also have a large service layer that comes in and does some of the manual checks, when needed. But for the most part, their work is automated.

**In terms of evaluating these organizations, how do you compare them?**

The objective of working with these vendors is to ensure that we're meeting requirements and maintaining trust and safety. In that situation, credibility is massive. We looked into which organizations were working with the vendors, reached out to those organizations, and made sure they ended up getting a certification and didn't feel like they had to rerun the process. In this industry, if someone says they're compliant with HIPAA and they're willing to sign a BAA (Business Associate Agreement), it doesn't always mean that they are complying with HIPAA and have a good HIPAA or PHI (Protected Health Information) manager.If you've been in the industry for a while, you know that you have to always confirm where a vendor actually falls. With a vendor like SecureFrame, it's really important that they've had success with organizations of different sizes and different scales and that people haven't had to rerun an audit again, either with the same auditors or with different ones.

I also look at whether we can use them for additional services. Beyond SOC 2, most of us are looking at GDPR if we're expanding internationally, or at California's state-specific regulations. There are all these different compliance checks that they run and we want to make sure that they're expanding their scope of service – not just focusing on a single compliance requirement.

On price, we immediately try to get quotes and that factors into the comparison. The big thing is that no matter what, the process takes a lot of time. With these compliance issues, it is actually a fixed amount of time. It takes six months to get your SOC 2 Type 1 certification. You can't get it in any less time than that, because the process involves one audit and then another one six months later. So, wasting time is the largest expense here. Therefore, it doesn't really

make sense to pick a vendor or an auditor that doesn't come with glowing reviews or evidence that they have helped many companies similar in type and size pass their audits.

In addition to these, you consider the quality of customer service. Everything involved in these audits is not going to be solved by software. You need a service representative on the other end. So with that, the level of attention and support became really important. So, we assess how quick vendors are to respond and how helpful they are when you're engaging in discussions with them, as well as how much they understand our use cases. For example, working with claims data from multiple payers can be very complicated and murky, so it was really important for us that our vendor knew what the law said. Our vendor knew what the payers' APIs were, and they knew standard protocols. They don't have to know the exact bits and pieces of the data, but they should be able to draw a flowchart of the data so that we can have a conversation to make sure we're protected. In our case, the biggest blocker to our getting claims data from anyone is our ability to pass their security audit – we might have a signed contract but the tech review comes at the end and could block us from getting the data we need.

One thing to note is that your vendor should ensure you pass not only the audits for certification but also what is usually a more stringent audit performed by your data partner or your data source. In summary, if you had a rock-bottom price but you didn't accomplish one of these other two things in terms of great service and a really reputable product that's served a lot of other customers that we trust, the price doesn't really matter.

**You didn't mention features or functionalities. Is that because the products are relatively commoditized?**

Yes, I'd say the options have become fairly commoditized. Note that this is where the difference between manual auditors and tech-enabled auditors comes in. The manual auditors don't have any integrations – they come in and sit down with you. You share your screen and they then go through everything. But with the tech ones, the features don't feel like they were that big of a deal. You look for what certifications they can manage, but again, everyone has landed on the same eight to 10 core ones. That's their bread and butter.

**Who all were you considering and how did they compare on these three or four key considerations that we've just talked about?**

There was a third vendor, Drata, besides SecureFrame and Vanta, whom we dropped pretty early. Vanta and Secure-Frame were relatively equal on features. Support from Vanta is really strong – probably stronger but in the end, the price difference was pretty substantial. SecureFrame was much cheaper. The end outputs as well as the reputability of both felt relatively similar. It felt like we were going to have to do the same amount of work either way, so we wanted to go with the cheaper product. We didn't feel like we were sacrificing on the potential of us getting a SOC 2 audit done in time. I do think that if we didn't have an engineer with the level of expertise they have, we would have probably gone with Vanta and paid more.

**Was it that SecureFrame couldn't provide that same level of support?**

Vanta's support is pretty phenomenal and they have a lot of experts on topics like AWS architecture, whom you can talk to about various things. If we didn't have our data engineer, who's our internal compliance expert, we could have used Vanta. You're basically trading on those expert hours – with Vanta, you essentially have a consultancy that's offering you a high level of support. I think it is worth the money if you don't have that internally, already.

I know a lot of people will say that Vanta's user experience is considerably better, but I don't think it matters. I can't imagine why that should be a determining feature here – in the end, if it does connect to all the sources you need,

and spits out a great report, the UX of the internal audit tool doesn't really matter that much. Paying for usability felt unnecessary. The tool is ideally something we only use once a month.

**How did you actually go about evaluating that? Was there some way of easily connecting the sources with them and seeing their outputs?**

You can do that. They've been pushing this option to set up a free trial and get a report, and if you want a detailed report, you have to pay. I don't think we did that. We didn't go and run the trial on each. A lot of our decision-making was fast (we wanted to pick one in a week) and based on reviewing their spec sheets, getting on the call with them a few times, getting their quotes, and then following up with any questions.

**What is the structure of their pricing and is it similar between both SecureFrame and Vanta?**

They typically price on a certification basis. They might also have some tiering based on the number of seats, because a SOC 2 audit is done at the employee level, so it matters whether you have five or a 1000 employees. So, I think they charge differently for different tiers of employer sizes. Say, I wanted to sign up for their SOC 2 product. There's a fixed base price that will get me the full certification.

If you just want the audit and maybe a review on the audit (not the full certification), you can pay a lower price. The reason why I think the certification costs more is that you need an individual to sign off and say you're certified. I forget if SecureFrame has an internal team for this or if they outsource this component to third-party auditors.

Vanta worked the same way, with the same structure as well. From a previous company where we looked into Vanta, I remember that if you went above and beyond, which meant asking them to assist with policy writing or in-depth research, they charged you for hourly consulting hours.

**What did the process look like once you had contracted with SecureFrame?**

They start with an onboarding and kickoff call with someone fairly technical on their side. On the buyer's side, that meeting usually includes whoever is going to be leading that audit internally on your side along with anyone else who's relevant. Usually, the people that are most affected are those running infrastructure and people teams, because that's where the majority of process changes that come up are focused. In the kickoff call, they talk through the process.

After that (although it could be before the call too), you start hooking up or connecting them to all of your different services. They help to make sure that you're adding all the right tools. Buyers might often not think to add a certain service because they're not sure it's relevant, but SecureFrame gives you guidelines on which ones you need to apply or not. The guidelines ask you the important questions – "Are you using a specific product for any of these different reasons? If you are, then you should hook it up. If you're not currently but might be in the future, you should hook it up." You don't want to have to rerun this audit because you massively changed your tech stack. So, they help you identify all the different services you need to hook up to their system.

After that, you run the audit, which happens pretty much automatically. All of that takes less than a week or two. After your initial audit, you can sit down with their team again to walk through it and understand what it means to implement some of the more complicated changes. They try to give you a lot of plaintext understanding and language to help you understand what the report says. There's probably some differentiation between vendors here too – I'm guessing Vanta gives you really detailed content and how-to's to help teams figure this out. SecureFrame was not bare-bones but it was lighter. At that stage, we had a bunch of questions about different methods of implementing a new change, and SecureFrame got on the call and answered those.

When we had implemented the changes, we told them and they checked and reviewed them. If there were any pending questions on either side, another call was set up. Up until when we got the certification, there was probably a call every month. There is no internal timeline on SecureFrame's end. They moved as fast as we wanted to move. They're not incentivized to help us move faster or slower. They're most incentivized to ensure we complete the audit, so we sign up for future audits with them.

**So they get onboarded, run an audit and recommend changes which you implement, following which they do one more audit, and then run the actual certification process. Does that capture the entire process accurately?**

They're continuously running the audit, with whatever can be automatically checked. If I have a new policy in place, for example, on personal devices, that comes up in the SOC 2 audit. As soon as I write that policy, SecureFrame picks it up and marks it off. It asks you if it has any questions, and you have to sign off on it. Those audits are continuously running and that helps you keep an up-to-date checklist of your actions. You might also review some pieces with them manually, if needed. This is more around questions like, "Do you have all your infrastructure set up?" They read your AWS site and check what is set up. For example, the tool said we were not set up with something yet, but we were. We weren't sure if we had set it up incorrectly or the system wasn't hooked up properly. So we got on a call with them and realized there was a small configuration change that was required.

**Could you clarify how you hook up your systems or services with theirs?**

Not everything has an API that you can just hook up. Some things do. With AWS, for example, you give it your AWS key, your container key or your cloud key, wherever you're storing different data. Then, you authorize the site to read it. It can go and read-access it. That's a pure tech integration type of connection. But there are also some types where you might just mark that you have an account on a platform where you can do some sort of single sign-on. In those cases, when they're saying you should be making a certain change, you just say you've made that change in the system. They don't know whether you made the change in the system or not, but they can at least make sure that you're covering your bases. This is because often, the checklists will tell you to do the same thing in five different locations, e.g., set up multi-factor authentication for all of your accounts. Some of those might be linked to SecureFrame but all won't be, but I know to go and do it, and can check that off manually.

**To summarize, what do you like most about the product?**

It does what it's supposed to do. This is one of those cases where it's one or zero. We either pass the audit or we don't, and we passed ours in time. It wasn't painful, and I've been through this process where it's very painful. It promised to be a less painful audit tool that got it done in time, at a fraction of the cost and a fraction of the effort. And it did exactly those things. The second thing is that it was really easy to get them on the line and get help when needed.

**What do you dislike most about the product or the service?**

It gives you a really long list of things to do. There are times when you don't have to do 100% of those things – you have to hit 90-something. I think their prioritization is good, but not great. There's a lot of nitty-gritty things that I wish were bucketed a little more appropriately, so it didn't feel so overwhelming at times. When you first get your audit list, it looks crazy. Maybe there's a usability angle here where they can better clarify which changes will take 20 minutes vs. two hours vs. three days. I don't know if that feature was there when we first used it.

**Do you feel like you made the correct assessment with SecureFrame?**

Yes.

**Do you anticipate continuing to use them for the next 18-24 months?**

Yes. If we end up going for a SOC 2 Type II, I can't see why we wouldn't use them. If we ultimately go for a HITRUST certification in a few years, that would probably require another evaluation before we went for it. The only reason for that is that HITRUST is a much more intensive certification and is longer. It takes a year. So, it would be worthwhile to do another evaluation to understand who's the best in that, because it's even more expensive to potentially get wrong.

**Is there anything we didn't cover that is worth mentioning? Anything you wish you'd known when you were making the decision?**

To go a little deeper on the service side of things, I appreciated that SecureFrame had a mix of expertise on their team, from technical to legal to business operations. They cover all the parts of the business where you might have questions around the audit. I almost always want a real person on these processes rather than how-to documents and infinite content, because the time spent looking through the content often ends up not being worth it. You also don't feel as confident. So, I appreciated how many support resources they have as well as that those support resources were experts in various fields and not just highly trained service personnel.