uberknowledge

Hema Lakkaraju, CEO, Ansa Solutions

Be as Innovative in Compliance as You Are in Your Business

Hema argues that compliance should be strategized and integrated to help it keep pace with fast-changing industry innovation.

02:09 What is a compliance strategy?

03:59 Understand the business, the market, and the product then create a compliance model.

06:03 The compliance mindset needs to change and embrace integration.

07:22 Compliance heads should want a more meaningful role.

14:10 Get educated. You don’t need to comply with all regulations, but you do need to comply with the regulations applicable to you.

16:48 HiTrust has included all the right things, but if it’s not mandatory, it’s toothless.

22:02 Build cybersecurity into products from the very beginning. Reverse reactive engineering is not the way to go anymore.

25:24 Compliance teams need to be mandatory within the design and product development teams.

26:08 You are answerable to the customers you design for, so build in trust and create value.

Ashwin Krishnan: [00:00:01] Good morning. Another episode of the UberKnowledge podcast. My guest today is Hema Lakkaraju, CEO of Ansa Solutions. Hema, for the benefit of our listeners why don't you give a little bit of your background.

Hema Lakkaraju: [00:00:15] Hi everybody. My name is Hema. I'm the CEO and Founder of Ansa Solutions. I have 10 years of experience in the life-sciences industry playing different roles from the development side and compliance side, especially focusing on IT and software compliance.

[00:00:32] I have recently founded a company called Ansa Solutions with the vision to demonstrate, communicate, and create compliance strategies for innovative life sciences. Our motto is, every industry has market strategy and business strategy, why not compliance strategy? Our organization is trying to drive that vision by collaborating the best of the solutions, best of the standards, best of the controls overall to meet the present high speed of the innovative life sciences industry and guide them with the appropriate compliance strategy.

Ashwin Krishnan: [00:01:13] OK, you mentioned two words that I've never heard juxtaposed before, which is compliance strategy. I've heard of business strategy, I've heard of financial strategy, and I've heard of personal strategy. Partly because people view compliance as a pain in the butt — something that I need to do to keep the regulators off my back — and you mention this, which I find intriguing. So, when you talk of compliance strategy, what is the immediate reaction you get? Is it, as we talked about yesterday, is it HIPPA, is it HiTrust? What do I do to just keep the litigators and the lawsuits off my back vs. what you talk about, which is much more holistic in nature. So, can you explain what you mean by compliance strategy?

Hema Lakkaraju: [00:02:09] I think, till now, we’ve had years and years of the traditional compliance model. If you go and say to a new compliance head, "OK you are hired as a chief compliance officer for my innovative life sciences industry.” What they first do is go and Google it and the first hit it comes to is HIPPA or HiTrust. They will try to take that framework and try to implement it. It might take one to five years and then when security or IT comes and says, "Hey, but you're handling people’s data and you have the IT component of it that needs to be implemented." Again, it goes to one to five years. Our major focus is why not try to understand the product first?

[00:03:04] I see a lot of gap between the compliance security teams and the products, innovative life-sciences products. They don't really understand what the product stands for, what its intended use is, and what kind of patients are they handling. First, if you're able to understand it better, work closely with the design and development team to understand the intended use of it, you can be a really core part of the team for product development. The problem that we have right now is people blindly going framework by framework and spending years on getting a product released.

[00:03:59] Rather, what we are saying is closely understand the product, what information it handles, what components it handles, and try to find appropriate regulatory standards. Whether it's NIST, whether it's ISO 27001, whether it's HiTrust most of those have 80 to 90 percent asking for the same controls again and again. Why are we not spending time understanding those standards, understanding those controls, understanding where your product needs to be in the regional area and trying to create a smart, lean client strategy which you can work on with the design team? In fact, you are not only creating a very safe life science product, but you're also going to market earlier than before. That's what we mean by a compliance strategy, why can't you understand it better, right? So, when you have a business strategy, you understand the business, you understand the market, you understand your product and then create a model that works better. Why can't we do that for compliance.

Ashwin Krishnan: [00:04:56] Again this is very refreshing to hear. I'll use the word easy even though it's not easy, but it's easy from a cognitive sense of I'm going NIST, or I'm going HIPPA, or I'm going HiTrust, even though, like you said, some of the controls, maybe a majority of them, may be common. So, you're actually taking a much harder route from a time perspective, but it's easier because you can just go look at a framework and say whether you've done it or not.

[00:05:30] Given your experience when you deal with clients, where does some of the resistance or push back come from? Is it more a people pushback of, OK, I follow a particular framework at least my lawyers are going to be happy, my board is going to be happy, versus me trying to work with my colleagues and trying to make this a core part of the life sciences product offering? What are some of the issues that you've encountered and how do you overcome them?

Hema Lakkaraju: [00:06:03] Typically, I define it as a mindset. The mindset that has been in place for years and years and years saying that you have to follow these regulations then you can look at the other aspects. But as time goes on, as the life sciences product changes, as the components need to become innovative, so does the compliance too to meet the needs. The reason of a medical device, how it has been manufactured or designed ten years back, it's not the same now. It's all about integrating: integrating with IoT components, integrating with the software features, some of the products. You have a combination of pharma hardware, software, and Internet of Things. If that has been innovative enough, your mindset also needs to be adaptive to the changes. Even though you have spent years and say we have mastered this, by that time your innovation has changed a hundred or thousand times and then it might be too late. You might have control on some things, but only some of the mandatory controls, not all of them.

[00:07:22] I think it's a change that has to happen to the mindset, especially on the compliance team. I would not say the CISO because the compliance team have to make that argument to the business team. But if you're going, as a compliance lead, to say it is NIST, I'm going to implement it. I don't think it's a very valuable position that you hold because what you are doing is something any management-level people can do. If it's just execution, how are you being a very valuable source to the CISO or any other manager? Your duty is to create strategy. As you have in any of the group, you have some people who create the strategy, who create the design, create the framework, and some people who implement it. Do you want to be in the C-suite in the compliance position just implementing the framework or do you want to have a bolder charter to understand the true nature of what the product is, what the market is, what makes this product innovative, and design it appropriately?

[00:08:30] I think that's the role that any compliance lead or executive level of the leadership has to do to go to market. If your product needs to go to the market earlier, considering the amount of competitors that you have, you have to take a different approach than others.

Ashwin Krishnan: [00:08:58] You bring up an interesting point because, like I said, this is the first time I've heard in any of these conversations about compliance needing to step above the traditional definition. So, in order for them to, even from a very personal perspective, to be market route, to be business route means not just interpreting the words in a framework and being able to just go do this and we'll be ok. Have you seen success cases where compliance officers have taken this approach and have become the key ally, if you will, of the Chief Security Officer or even the product groups? Where they are looking at this and saying, “Hey by doing this, inherently my pacemaker or my insulin injection is going to be a much safer environment. It's going to be less prone to hacking. It's going to be less prone to Denial of Service attacks.” So, have you seen certain industries within healthcare which are much more forward leaning and are willing to embrace this proactive stance on behalf of the customers?

Hema Lakkaraju: [00:10:23] Slowly the ripple effect has been happening, where we see at multiple conferences CEOs talking about habits. How that defines a company and that can also demolish a company, which means people are starting to understand the value of information, whether it's a customer or patient's information in healthcare or an employee’s personal information inside, that ripple effect is happening. But even though, I see a lot of resistance from the client’s needs. So, we had some cases where if we propose to an organization saying, "Hey, think on the higher picture," and they say, "I don't want anything to do anything with that, just execute this once.” Again, I think the starting point is going to change the mindset from a compliance lead perspective so that they can have the ripple effect from the CEO. We have been in projects where we have taken a multi-angled compliance approach and even though it faced a lot of resistance from the traditional compliance leads, overall when we went to the audits, they didn't see any of the flags and that gave them a reason to object to it saying that's what the hybrid model does. We are trying to knock off in a small amount of time as much as you can be compliant with.

Ashwin Krishnan: [00:12:03] It's almost like what you're saying is that there is certainly a human element to this which is if I just follow the letter of the law, in this case the compliance law, I'm not going to lose my job. But if I stick my neck out, yes there is potentially opportunity for me to become a much more strategic thinker and be part of the business, but there is also the risk of somebody coming and saying, "Hey what are you doing? Why are you interfering?" If I'm the business owner and the compliance officer comes to me and says, “Hey by the way, you take these controls, I have a road map to deliver against, I have competitors who are nimbler.” Clearly there is a "risk" the compliance officer is taking, but based on this conversation what you mentioned is the bigger risk is not doing that because at that point you're putting the business at risk by not doing your job.

Hema Lakkaraju: [00:13:01] And it's how you present it, how you present it to the business owner. I have seen a recent article by the governance risk and compliance lead saying, now more than ever create a business risk to the CISO in terms of the need of government risk and compliance. And I would say it's how we communicate. If you communicate in a way saying, I create the strategical model but this strategical model has been driven from these applicable standards and regulations.

Ashwin Krishnan: [00:13:33] Right.

Hema Lakkaraju: [00:13:33] This is the pool of every person's controls that we are talking off. People are willing to buy in, but if you say I just created a strategical model for compliance not telling the history of it, then it's going to raise flags.

[00:13:50] And the important thing that people always try to ignore is what our standards and regulations are. They are at a very high level. They don't tell you any detail ever. They say security by design or privacy by design.

Ashwin Krishnan: [00:14:07] They say zero trust.

Hema Lakkaraju: [00:14:10] Yes. They say vendor management is choosing the vendor by its intended use, but nobody ever goes into the next level of detail because it changes organization by organization. And that's where the compliance lead comes into position, where they look at these regulations, look at what is actually applicable for my organization. Not all regulations might be applicable to my organization and if you blindly go regulation by regulation not understanding its intended, its scope to your innovative life sciences product, then you're actually wasting your resources and time and its overall business risk by not going to the market.

Ashwin Krishnan: [00:14:51] That's a great point, the ability to customize what's needed versus what's not. So, let's talk about the regulatory community and we are at the IoT, blockchain, AI, cybersecurity summit here. California is probably at par with or even leading the European Union right now when it comes to forward-leaning regulations and they have some pretty advanced IoT regulations that have come into play. So the question is, coming back to the regulatory environment we're in right now, do you see awareness?

[00:15:37] So, California as an example, in September 2018 they passed a pretty expansive IoT regulation. Simple thing and we take it for granted, but a lot of IoT hacks have been happening over the many, many years, and maybe even decades, about having default passwords for every device. So, what seems like a fairly trivial item has not been codified. Every IoT manufacturer starting in 2020 has to have a different default password for every device they manufacture. And you and me as consumers, when we boot the device up first time, we can't even use it unless we change the password. It seems very small, but now you have a regulation in place it automatically raises awareness for IoT manufacturers which may not even have a tech background, they could be healthcare or something else.

[00:16:33] So do you see that happening in healthcare where there's a much more activist role that federal government or state government could play which automatically raises the awareness level.

Hema Lakkaraju: [00:16:48] I think it's a very good question but at the very right time. I have been looking at the HiTrust, the new version that's coming into market and it shows how much proactive the HiTrust people are. They are taking the next new version into consideration. They are taking the new finance regulations into consideration. They are taking the new privacy by design also into consideration. Which means that what while we have some of the greatest standards, that are trying to make themselves more holistic, as I was saying, but it is not mandatory, it's kind of nice to have. So, HiTrust will get the certification but it is not equal to the regulation.

Ashwin Krishnan: [00:17:38] So why do it, becomes the question.

Hema Lakkaraju: [00:17:39] Correct. And that's the great step that the EU have taken, the initial step of making GDPR mandatory. It's something that we need to do for the innovative life sciences as mandatory. Considering how innovative and fast healthcare is growing, we have to at least create the basic framework of the basic controls and making sure that those basic privacy, security, design controls once done are not radically impacting the final patients' data.

Ashwin Krishnan: [00:18:16] And that aspect of this is something I've heard from lots of people, even when it comes to GDPR, and is exactly what you were saying earlier. There is a definition that's in place. Let's take one example, the right to be forgotten is one example of patients or consumers being able to exercise their rights over their dormant data. Now, that's at the highest level. Going down, it is this primary backup, secondary backup, tertiary backup, that's data deduplication. There could be more groups that have been built on the data and influences and predictions that have been made. Do they fall into the data destruction? There's a lot of these implementations.

[00:19:07] So do you see an opportunity for that also to be something that the compliance officers can now start filling in because these are very wide regulatory frameworks with big financial impacts. What does it mean for us? What does data destruction mean for us? This patient data that could be for cancer research. And if I, as part of the survey, could come in and say destroy my data, how do you interpret that? There's a greater good to be had. That's one example. Do you expect more of that? California is taking a much more active stance. We've seen what's coming from GDPR, but it's going to be different in different parts of the world. States are probably going to vote on it. So just getting your head around, if you're a global organization, what is relevant for me, which one should I implement? To me the definition of the role of compliance officer getting much more complicated.

Hema Lakkaraju: [00:20:22] It's getting much more complicated. At the same time it's pushing the ability and the skill set that a compliance officer has to accumulate. If you are a life-science industry compliance officer or a quality director, maybe not entitled to understand the life sciences security, not entitled to understand the data science, but now it's at the C-Suite you have to push that skillset saying that this is what our product stands for. This is what our organization stands for. Better get your skill set and knowledge around that one. Only until that skill set has been filled and the awareness has been done from a C-Suite level of compliance and quality directive to understand the overall arching line of what is the data value, what's privacy, what's GDPR, what is insider security – how does it all fit in to my product and my organization and what it stands for.

[00:21:30] I don't think even a C-Suite level quality or compliance director can fill in the role. As you said, if they don't understand the business model at all, they collect the data and the customer or patient asks to delete the data and, without understanding how the operation works around data, he may just say yes. But he will be questioned again, asking why is the data in the first and second backup.

[00:22:02] I A big part of the ignorance is the silos that we see right now, the major concern that I and my organization have, is people working in silos. If you get hired as a quality leader, if you get hired as a quality director in the life sciences industry, you work with your teams who are from a traditional mindset and work on the product design, on a clear set of rules or if it is a medical device – 62304 and 13485. But if it is integrated with IT, when are you going to reach the CISO to talk about cybersecurity? Until it's almost ready to the market?

Ashwin Krishnan: [00:22:56] It's too late at that point.

Hema Lakkaraju: [00:22:58] It's too late at that point. And then you have to do the reverse reactive engineering to fill in the gaps. That's not how we have to go. The need for collaboration is higher than ever. Either a quality leader or director should embrace that they have some lack of knowledge around cybersecurity and so on and get used to it or work collaboratively with the CISO to understand and create an integrated holistic model so that you keep your patients' data integrity, compliance, and privacy because there is no business without the customer.

Ashwin Krishnan: [00:23:39] I think it's a great parting shot. Any final words? I know we've covered a lot of ground, the compliance strategic officer, their role in the business, and the silos, and how they need to think about the business. Any big takeaways from this conference? I know you've had some great conversations. Anything that stood out or reinforced some positive vibes that you already had or something that scares you?

Hema Lakkaraju: [00:24:15] I have kind of mixed reactions. If you talk with the development head or the business development head at this conference and ask what is your compliance strategy, their immediate reaction is why is somebody trying to understand the product, right. If you talk with some of the VCs I've talked to today and yesterday, they are like, finally somebody tried to understand this better because we are going in loops and loops and loops of being compliant, and we are never able to reach the mark and it's not good for the business. We are not saying that you need to bypass the regulations. What we are saying is, as you are innovative in life sciences also be innovative in compliance because if you're just executing to the frameworks, that's not what the C-level executive suite is actually capable of. They are capable of bringing their skill set and experience understanding the product.

[00:25:24] The major concern that we see right now is having that gap and changing of the mindset. Compliance is never an absolute outside supporting system for an organization, especially when you to come to the product design and product development. It needs to be mandatory teams inside the product development. At the same time, we see the development teams trying to just look at checking marks for compliance, but they have to also understand that you are answerable to the customers you design for.

Ashwin Krishnan: [00:26:01] I think ultimately, like you're saying, it could actually end up becoming a big competitive advantage and building trust with consumers.

Hema Lakkaraju: [00:26:08] If, when you take your product to the market, you actually took all the steps by including privacy in design, security by design, put cybersecurity for medical devices best practices into place, and created a holistic tool then people don't need to come back and ask for constant updates or I'll wonder if I'm not so sure about your product. Just build it in and show we are trying to maintain that integrity and the trust you have in us. I think that will give you a sure shot higher value compared to competitors.

Ashwin Krishnan: [00:26:49] Got it. Amazing conversation, Hema. Thanks for being on the podcast. Looking forward to further conversations.

[00:26:57] Thanks, Ashwin. Thanks for your time.