

Questionnaire – Demographic Questions

1. What is your current role in the company?

Software development

2. What kind of tasks do you usually do in your work?

Fullstack development: backend and frontend and a little bit of infrastructure. But not that much because [redacted] is doing all that. But I am taking part.

3. Given enough time, can you understand the architecture of an application system that is described using an IaC script of an IaC technology you are familiar with?

Yeah. I think so.

4. For how many years have you worked on tasks associated with IaC tools?

I would say for four years.

5. How large is the company you currently work for?

< 50

Questionnaire – Compliance Rule Modeling and Checking

6. How do you check the compliance of the software applications of your company?

So, I mean, there are different stages of compliance. So, maybe the most low level is just checking code. You can call this compliance, but we use PSLint or Sonalint stuff and stuff like this checking, and on the infrastructure levels of Kubernetes, we don't have automatic checkings: So, this is done by us (...) by manual checking and looking. You have in the video, there was this example that certain users only have access to the database. This is checked manually, but we don't have automatic checks. It (doesn't) bother us and our company is way too small to handle this.

7. Do you use well-defined models for the compliance rules applicable to the software applications of your company?

At the moment, none, yeah. It's just in probably in our heads, as best practices. And I also have to say that at this point that mostly one person is doing this. One or two, so me and [redacted] the most time. So, we'll talk about all the cloud infrastructures or spinning up databases or using the service and managing the Kubernetes. I think this is more in our best knowledge, but we don't have written it down.

a) If so, how do you define them?

8. Do you think having a well-defined and machine-readable format for compliance rules reduces the complexity associated with checking them?

Yeah. I think so, yeah.

9. Do you think having a well-defined and machine-readable format for compliance rules reduces the uncertainty associated with interpreting them?

Yeah, for sure

(For) question eight and nine, I can totally imagine that this is, like, super useful, you know, especially on a large scale. If you're a large-scale company, and just some people define those rules, and then, yeah, they automatically check, for example, if other guys want to spin up for them or something, and then they automatically check if the settings occur to the predefined rules. It's very useful, I can imagine. But, yeah, we're not at this stage. For us, it would be a waste of time, because we would put so much effort from that stuff. So, maybe, in another stage, it's more useful.

10. How often do you have to deal with new compliance rules?

Zero times.

11. How much do you agree with the following statement: *using IACMF reduces the effort associated with defining and checking compliance rules?*

So, defining was a little bit of question for me. You also had to, always had to first define your rules in this Job thing, right? And then, you can use some templates or plugins, but they seem a little bit minimum, and you still have to define your own logic. So, the question, which came up to me was, I think this tool is powerful (but only) once you have a big market place where we can (re-)use the stuff you defined in the video: it's just shared, and you can already use it. So, you use this null-checker and you don't have to write the bash script yourself. It's just there, you can use it, and then it's super powerful. (In) the video seemed a little bit long to come to the stage where you finally can check something.

(Ghareeb: So, you say if you have kind of a marketplace that already has pre-configured compliance jobs, this would make the compliance rule definition part easier, right?)

Maybe not jobs, but those plugins here (and) I wouldn't call it marketplace, because you don't pay money for it, but it's just a library full of those useful things. As an example, I mean, if you take ESLint or something, some Linter, you can check which rules, they always have a set of rules, and you just say you want them or you don't want them.

(Ghareeb: So, let's imagine two scenarios. (i) If you do have such a repository of plugins and pre-configured plugins, and (ii) if you don't. So, let's say if you do, what would you choose on the scale?)

Four

(Ghareeb: and if you don't?)

Two or three. Let's say three. It is in the middle.

What I also didn't like is this... I don't like UI stuff. So, what I expect as a developer is as-code. You can define those compliance rules in YAML or something as-code. I think there are also existing tools. But I can't remember the name. So you can define it as code. It's also called, I think, compliance as code. You define your compliance rules. Just in code, like you would define the infrastructure. And this would feel a little bit faster for guys who are already aware of infrastructure. They don't have to click through the UI. I think this is also just implementation details. I mean, imagine something like you have a visual studio code plug in, and then you can nicely, like, sketch (the compliance rule) into your code, and then you through the file against your API, and then it just works.

And I also forgot the effort for checking. I think once you have your job, really asking (the framework) to (perform) checking, is no effort. This is really nice. I would say, totally agree: It reduces the effort.

12. How much do you agree with the following statement: *using IACMF reduces the complexity associated with defining and checking compliance rules?*

Complexity in defining, I don't see that much, to be honest. I mean, at the end, it is the whole idea. You shift the complexity to defining your rules. But when you define it, it's no complexity during checking, because you have your rules defined as machine-readable instructions.

So, defining, I would say, it's still complex. So, the complexity defining is a would say two.

Checking is, yeah, I agree. It reduces. So, five.

13. How much do you agree with the following statement: *using well-defined models for compliance rules reduces the uncertainty associated with interpreting them?*

Yeah five, I would say.

Questionnaire – Architectural Reconstruction

14. How do you reconstruct the architecture of running application instances you need to understand?

(For Kubernetes) we use Argo CD, so this is one thing to visualize all our containers in running in our Kubernetes cluster. This is always the first thing I do when something goes wrong with our cluster. So, you go there, you see all the information of all your containers, which ones are running, which version is deployed, so you can see at the Helm and chart, which is deployed, which container image, or the resource annotations, so you get a pretty good overview of the current state of your services, (but) this is only covering Kubernetes, so what is not covering is the whole view. I don't know, other databases in the cloud, or some queues, or whatever.

So, for the whole view, I need to go into Google Cloud and check what is up and running, so we don't have an overall view of this. So, I would go there and check.

15. Do you use any (semi-)automated tools for this purpose?

(Ghareeb: so you do use an automated tool, but partially, right? Because you have a tool that works for Kubernetes, but if you want to get an idea about external systems, you need to do that manually, right?)

Exactly

16. How much do you agree with the following statement: *using IACMF reduces the effort associated with reconstructing the architecture of running application instances?*

So, if it works like a charm, I would say five. I mean, the idea is nice: One central tool where you can visualize your whole landscape. Yeah, and if you have to implement plugins, If you have to implement it yourself, it depends on how easy and how well documented the API for Google is, and what credentials you need. I would say three or two.

But the good thing, I think, is when you do implement it, it becomes very efficient, right? Then it's super efficient, and then again, hopefully you can share it with other people. In the best case, some other poor guy has already implemented it. I mean, this is the most important part for frameworks like this. You need a community who creates those plugins, and then it's super nice.

Questionnaire – Compliance Violation Fixing

17. What do you do if you find out that a running application instance violates a compliance rule?

Probably I would fix it manually. Let's say, let's construct an example. Let's stay in this Kubernetes space, so I find out that one container exceeds the maximum amount of CPU. This could be a case. So I would go in our Helm chart and fix the code: Eight CPUs are not allowed but you now use four, and I deploy it again and check in Argo CD if everything worked.

(Ghareeb: if you find some managed service, let's say, from Google Cloud, that has a violation. How do you fix that thing? also in the same way or do you do it some other way?)

There we really, everything is (done) manually. So I guess there would be something like Terraform would be handy. Let's give you an example. We use BigQuery and this is like a data warehouse from Google Cloud where we will put all our metering data from our usage-based metering. But this is all configured by hand. So if they are, for example, something goes wrong, we don't have it configured in code. We need to configure it again. Everything manually created: Create a new database, create the queues to put the data in there... So this is not written down in code. But we also don't have any compliance checks. And if there would be some compliance issues, let's say, for example, the queues are wrongly configured, we would look at it in the Google Cloud and configure it with a UI.

18. Do you use any (semi-)automated tools for this purpose?

(Ghareeb: So you do have automated tools, which is only applicable for Kubernetes cluster. But sometimes you have to do things manually, right?)

Yeah.

20. How much do you agree with the following statement: *using IACMF reduces the effort associated with fixing compliance violations?*

I would say on a large scale, yes, on a small scale, no.

So, if I only have three services, I think it just introduces more complexity. One thousand services, probably it can reduce the complexity. I'm sorry, effort, effort, yeah. So let's imagine I'm so like we are a small startup and we have only five cloud services. So five cloud services is super easy to handle manually. And I think the complexity to introduce a framework like yours to just fix potential compliance violations would be more complex than just do it manually. So if you have a small scale, I think there's not much benefit. So the effort is bigger to introduce, you know, your compliance checking framework. But if you are a big company, a lot of guys, a lot of services, I think it's... I can see that it reduces the effort. But I guess here again, it depends on the size of the company. And also on this amount of services used. I mean, you could have many services while being small, of course, small company. But the size also means like many, many people that needs to do the stuff, right?

So in our company, we have two guys, and it's super limited to the amount of people who can do something stupid, but if we onboard every week, new people, and I guess it's hard to handle to educate them on the same level and to ensure that they all act in a similar way. I think that it's super useful to have something like this.

21. How much do you agree with the following statement: *having well defined models for compliance jobs reduces the uncertainty associated with handling detected compliance violations?*

Yeah, I would say five.

Questionnaire – General Questions

22. How do you evaluate the novelty of the framework?

it's hard for me to say because I don't have that much knowledge.

So what I know is from the research I did is that there at least some sort of, like I said, this compliance as code where you can define something like this. You can define rules in code for your infrastructure. Maybe you can really define something like only those users for the database or the location. So I think this already exists.

What I haven't heard of so far is this automatic repairing. So your whole process. At least for me it was something new. So you detect it and you fix it all at once, and in a perfect world, this works perfectly. It fixes everything.

I mean, the idea, it's super cool probably.

23. How do you evaluate the extensibility of the framework?

I see this trade-(off) between academia, you always want things super extensible. In business, I don't want this. I want to use something that already exists. Yeah. And everything should work out of the box. I don't want to care that much about extensibility. Extensibility is for edge cases, but I hope that I don't reach those edge cases because when I buy stuff, I expect that it just works. So this whole extensibility, in my opinion, is not that important for stuff like this because you choose such solutions because you don't want to care about it. So the last three years, I never thought about extensibility.

You can extend it with the plugin system. The idea is nice.

24. Would you use the framework in your work?

So in our stage, no. In the later stage, if it's more self-contained and I don't have to do much, I just take it and say, give me those predefined security checks and then just, I can, I don't know, put it in my CI/CD and it runs every time you push and fix automatically all the issues, then yeah.

If people have to work on it like a month to get it working, probably not.

a) If so, in which areas?

25. What is your general impression?

So the idea is nice there and it depends on how easily and this is, I think, is always a problem. How easily can you integrate it in existing solutions. It's the tooling question. If there's nice tooling around it, it's great. The overall idea is nice.