

Questionnaire – Demographic Questions

1. What is your current role in the company?

Research software architect.

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

UM's on the one hand, providing blueprints for applications like kind of meta architectures and other things like normal, we research work.

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

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

12

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

< 100,000

Questionnaire – Compliance Rule Modeling and Checking

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

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

I would guess these are just **simple scripts** or **simple Python things**. Then like like the CI pipeline I would I would assume it happens in some **CI checks** (...) Would I would bet it's more like this really. Really scripts, because we've got dozens of security experts and and also then putting focus on **automation**, we even have a security expert in research so that each research is is, is, is secure and follow some rules there (...) the checklist I just opened was just a simple, **simple checklist** (...) There is a Jira ticketing system where the checks of the system are inside here and then if you work in a new system you just copy the Jira tickets and then you have to check that at the end all tickets are resolved. But plain text.

- 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?

Yes, sure.

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

Yeah yeah I would say partially. How do I know that the script written there is correct? So how do I check the compliance rules for quality? Quality meaning also meaning being correct with respect to the requirement. Can it be with your MySQL example that the system is configured

Kommentiert [GF1]: Simple scripts, simple checklist, and Jira ticketing system

strangely so that the rule says everything is OK but this there is maybe some other MySQL instance (...) and the compliance rule comes in and checks version 1 only. Can I be certain that checking (covered) everything?

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

I don't know

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

Defining. Depending on the quality measure of or what the company has for the for for compliance rules (...) There are some text being there (and) in a novel workflow you say "Use that rule, end of story" And this is a very easy thing, and if I now use IACMF, then It's like effort without end **so I would disagree.**

For checking for sure. The automation is great and also the topology reading because if I spend effort in the thing and I've got 100s of applications as a security office or whatever, and I have got a nice overview: in this area there are more red flags. Like the approach one uses with source code quality checks with SonarQube. Automation really helps **so I would put up four.**

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

Ideal World One writes Python scripts or bash scripts and and and fires them up and has a self-made pipeline, maybe with some output. What is still possible with your framework because I can stick in arbitrary Bash scripts and kind of stick in arbitrary things and I've got some structuring on my rules because this strengthens the structures and guides, and **so I've got not some wild west growing but the framework gives a structure, which reduces complexity.** Okay, and I'm deciding between three and four. So I gave it, I gave it **a three.**

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

if "well-defined" is only syntactically well-defined without any quality check around, then it's like three or four.

(Interviewer: So you say what's important is not only that the rule is well-defined but also how you come up with the rule?)

The process and then also the feedback: like the guy can improve the rule. **Then let's give a three.**

Kommentiert [GF2]: The rule before the introduction of the framework could be much simpler! So defining the rule is not easier.

Kommentiert [GF3]: The rules themselves could be not completely trusted. In this case, uncertainty is only partially reduced. It is important to have a cooperative process for defining the rules that includes discussion, checks, and feedback.

Questionnaire – Architectural Reconstruction

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

Pen and paper and some manual investigation and calling to colleagues. A backstage could be an example like a Spotify Backstage instance running and now I want to know what is the database and so on and now I need to go and it's like checking manual checking of the CI scripts manual checking of the running instance if I get the ssh key to go there, and so on.

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

I don't use any because I'm not.. because I think the effort of running.. **finding and running those tools is not worth it.**

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

What I had in mind if I have thousands of instances, are they merged together? So maybe I can see what are the differences and commonalities because if I've got thousands of separate things only being different in the IP address of the host, what does that help me? **It helps me seeing the single instances, so for the question itself it will be five** but it doesn't help me in a post processing.

Questionnaire – Compliance Violation Fixing

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

Manually going there and I don't use any scripts.

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

I don't have any automatic tools.

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

The demo showed some really code-near things, but if the compliance rule is like "you need to have two-factor authentication from next year on", this is a complete rewrite of the user login thing and then thinking how are tokens are sent to the mobile phone and which app and this is a really architectural thing and one needs to do much things, so the framework doesn't help at all in that case because there's no way yet, but for the simple rules as you showed like don't have an admin login running there for the production system or for the testing or for the integration then it's great, great stuff so I would stick with it partially, because it depends on the rule (partially was earlier interpreted by the participant as 3).

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?*

I would put a four. Why not a five? Because there are, besides the uncertainty of the of the fixing itself, there's the uncertainty of is this model correctly done. You know, if I have 1000 checks there, how can I be sure the the whole thing is correct and it covers all cases? right?

But it provides structure because like it provides a set of interrelated compliance rules (...) because (they are) in the same application. One has some, like, feeling of the of the application so I think that it's a four.

Kommentiert [GF4]: For some complex rules, automatic fixing is not possible, for simple rules, it is great.

Kommentiert [GF5]: There could be uncertainty of the quality of a compliance job, but a compliance job gives structure, which reduces uncertainty.

Questionnaire – General Questions

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

There is this GitHub **Dependabot** thing, and I was checking **SonarQube**, which also could be a thing, then I also saw this **penetration test**.

But what I did not see or stumble over a framework combining all of these things because the cool thing of the framework is okay, I can be at the lowest level and at the highest level and I could do anything but I've got a defined pipeline and the defined reporting structure. Being domain-specific for compliance checks even. Although I said at the beginning that **there could be some CI checks running** and so on but this is the most possible general framework and it's like I have to have the mental mapping from the CI checks to the compliance rules somehow with some things and this and the framework does that for me, and then I can also have more coding-far-out people using this framework like knowing security very well and then these persons can sit together with experts coding the rules, but the security experts can read the thing without calling an expert hey, what does the CI thing mean? because the UI.

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

This is the core idea of the framework and the core achievement and I think it's what I did see here was great.

24. Would you use the framework in your work?

Yeah, I would try it out and I would be curious what are the limitations of the rules themselves.

a) If so, in which areas?

I would include the framework in the meta architecture and use it as one check that the architecture is good so like if someone starts coding and implementing things and then the framework should report if our rules are held and so on (...) so no fixing.

25. What is your general impression?

The meta model is good to read like how to collect rules and the jobs and the fixing and also the architecture and also the pluggability of the of the importers they do not rely on TOSCA you're relying on anything you just have to have some importer.

But in the details we see that it's a research prototype. And you know like (you need a) more proper UI thing, but on the other hand this is checking compliance rules this is always effort and it's always work, it's not easy like I spent 10 minutes to do something and then I'm complying now it's a huge work and your framework reduces this work especially by structuring things.

Kommentiert [GF6]: Some other tools can solve certain compliance management tasks, but the tool does it all, and gives structure. Also being domain-specific is easier for non-experts.