**Transcript: *Interviewee 1***

May 13, 2025, 1:00PM

 **Interviewer** started transcription

**Interviewer** 0:17  
Hello, my name is Bart  
For my Master’s thesis at the University of Amsterdam I am conducting a research project in collaboration with Kouters van der Meer, where I’m researching the process of how companies or organizations evaluate and adapt their Internal Control Frameworks based on changes in legislation or industry standards.  
I'm studying how it's being done currently, at least theoretically, based on the popular frameworks like COSO, COVID and ISO31000. The goal is to find out how Artificial Intelligence can help that process.

**Interviewee 1** 1:09  
Mm hmm.

**Interviewer** 1:11  
So that's what why we're here.

**Interviewee 1** 1:12  
Mm hmm.

**Interviewer** 1:14  
For the interview first, I'd like to know about your personal experience in this field.

Then I'll show you a pipeline I’ve developed of how ICFs are theoretically evaluated and adapted.

**Interviewee 1** 1:23  
Sure.

**Interviewee 1** 2:21  
Yeah, sounds good.

**Interviewer** 3:04  
All right.  
Well, then the first question is, is for myself to get a better understanding of you and your context

**Interviewee 1** 3:09  
Mm hmm.

**Interviewer** 3:10  
Could you maybe introduce yoursel, your background and your experience in this field?

**Interviewee 1** 3:15  
Yeah, sure.  
Yeah. My name is [NAME].  
I'm originally from [COUNTRY], but yeah, I've been here for long enough to become Dutch, at least on paper.  
So I have the Dutch passport.  
I’ve been working in IT for like more than 15 years now.  
So my whole professional career.  
Before that I studied at the Electrotechnic University in Bosnia, I studied telecommunications and I finished my Master's degree as well.  
That was all before I moved to the Netherlands. I worked for six years in in two different IT companies in Bosnia. And then I got the opportunity to work in a different company here in Amsterdam.

The company was called [COMPANY NAME], they build software for large bank and financial institutions. They're quite big now.  
I think couple of thousands people spread around the globe.  
After that I I spent five years in a company called [COMPANY NAME].  
I advanced my career from like system engineer all the way to head of infrastructure at [COMPANY NAME] and that was 2 and a half years ago when I moved to [CURRENT COMPANY NAME] to become their IT manager and then I was promoted to the head of IT department.  
So that's what I do. So as I mentioned, yeah, my whole life is is has been around computers.  
So initially you know you start as a kind of support engineer and then you advance to like System Administrator. You know then I specialized with infrastructure but also you know database, server administration, network administration, that all falls under the the system engineering.  
Yeah, before deciding to to move into kind of management role and and yeah now I'm head of IT and yeah responsible for pretty much anything.  
That has to do with IT at [CURRENT COMPANY NAME] and yeah, quite enjoying it so far.

**Interviewer** 5:39  
So that's a very technical background.  
And then later on you move into the management side?

**Interviewee 1** 5:42  
Indeed, yeah.  
So I mean that's kind of also a logical step.  
You know, you climb the ladder as as you progress because yeah, for more than 15 years, I was mostly hands on and, you know, especially in this company it was more like, you know, bare metal infrastructure, you know nothing related to cloud because [COMPANY TYPE] are competing in this, you know, low latency space.   
So you want to have everything you know, as close to the exchange as possible so you can do the the trades faster.  
But then yeah, since moving to [CURRENT COMPANY NAME], everything is shifting to cloud and now with AI, we will see.

**Interviewer** 6:33  
OK. And and then Internal Control Framework themselves and risk management, how experienced are you with that would you say?

**Interviewee 1** 6:40  
So I had to do some things, but I was not directly responsible for IT in the previous job.  
So the last, six or seven years, but yeah, since moving to [CURRENT COMPANY] and taking this role of head of IT, I'm more and more involved, actually I'm directly responsible for the IT part of the risk management.

**Interviewer** 7:06  
Mm hmm.

**Interviewee 1** 7:08  
We do what we call the risk management life cycle or [*UNITELLIGABLE*].  
Self-assessment cycles every year, so we assess different IT related risk among all other risk as part of our enterprise risk management framework altogether. Yeah. So we identify the risks, assess them, you know, for probability and impact, grade them and then create a prioritization. We accept what we can accept and deal with what's not acceptable for us in the best way that we can. So either you mitigate or you take some kind of an insurance or you transfer the risk to other parties and so on. But yeah, risk management became a bit more of our priority, since DORA basically kicked in. DORA to me is all about, you know, managing these risks, obviously on a different level because yeah, with this supplier management part of DORA, you have to manage not only your own suppliers, but also kind of dig into the their chain.  
So you manage well, you don't directly manage, but you need to have oversight of of suppliers of your suppliers, so you know the chain goes on and then.  
Yeah, I have a feeling that with DORA it, it's gonna put much more structure in into not only the risk management, but you know, to me DORA, is now just common sense. It's nothing new. It's just that they want to apply, you know the the same or more or less the same rules for all financial institution.  
But what we struggledwith a little bit, at least in the beginning, while DORA is not yet 100% clearly defined in in all aspects, you know to me it does not make sense to assess the firm of, you know, 20-30 employees. You know, some funds are even smaller than. That, and let's say ING bank or or ABN Amro or you know those big players that have 20,000 people. You know it was funny, I have a colleague that works in in one of these big banks. And I asked him, OK, you know what?  
What are you doing to to get yourself DORA compliant? And he's like, oh, yeah, we have a team of about 50 people working like, a DORA working group, you know, and I have 42 employees in in the entire [COMPANY].  
So yeah. So I mean that that says something about the scale as well.  
But hopefully you know the the auditors when when it comes to to that part will have that this kind of you know proportionality in mind.

**Interviewer** 10:01  
Mm hmm.

**Interviewee 1** 10:01  
With DORA, if you look at the the regulation itself, like the structure of it. So let's say the level 1, the regulattion itself talks a little bit about proportionality but it doesn't define the specific criteria, So is it the amount of money that you're dealing with, or is it the amount of people? Is it the amount of branches that you have? You know what is it that defines the proportionality? However, if you go to these RTS and ITS documents., they were considered as kind of level 2 regulation.  
They you simply lose this, you know, proportionality.  
Basically, everybody needs to do everything unless you are, you know, very small, firm and then there is a simplified framework and all that.

**Interviewer** 10:39  
Mm hmm.

**Interviewee 1** 10:47  
Yeah. So I think Dora is is a good step. I always say it's not reinventing the wheel.  
Everything the Dora prescribes, it's common sense.  
It's what you should have if you're a serious company, you know, especially working with finance, but you know it’s gonna take some time to evolve it in a way that you it makes sense for smaller companies. But it was the same with all these bigger regulations, the same happened with GDPR a few years ago. Initially they said, yeah, you're gonna have to do need to do this and that. But then, a few years later, you know it's all about, you know, classifying who's your data processor and who is the owner of the data and and what's happening with it and make sure that you know where it's stored. That's all it is.

**Interviewer** 11:40  
So in the beginning it's a very overwhelming thing, but if I understand you correctly, as time passes, it changes and starts to make sense?

**Interviewee 1** 11:47  
Yeah but also, I’m not sure how involved you personally are with DORA itself because you know let's say two years ago they initially published the the first draft and then they go back and forth with, you know, updating it that they said there are 5 pillars.  
So basically you know the the the risk management framework with all these policies and procedures is one of them. Then you have you know, testing, you have incident management, you have supplier management and 5th one is about sharing the information. I mean this is all from the top of my head but yes.

**Interviewer** 12:26  
Mm hmm.

**Interviewee 1** 12:28  
Now, when DORA kicked in, basically it it went down to two things.  
One is the incident management so that they defined like how you should submit your incidents. So there's a clear form, you know there are 50 something fields that you have to submit in in case of a major IT incident.

**Interviewer** 12:41  
Hmm.

**Interviewee 1** 12:48  
So that's one thing that they care about.  
And 2nd is the supplier management. So basically they went down to two things that are important. Nobody's asking you about the risk management framework itself, which is consists of at least 40 different policy and procedures. I mean, maybe they will come at later stage and assess you if you have all of these policies and procedures in place, but so far in it has kicked in, yeah, maybe four months ago or something. Nobody from the regulator side asked anything about any of these other pillars. They only care about incident management and the supplier management. Actually a month ago we submitted our own supplier management register. It's called information Register, but it's basically information about all of your suppliers and then the suppliers of your suppliers and so on.

**Interviewer** 13:44  
Mm hmm.

**Interviewee 1** 13:48  
So yeah, I think it's still a long way to to evolve.  
I mean the idea behind it is good, it's just that they have to sort out some of these major things, you know, like proportionality. Different things for different, you know, types of financial institutions. It's not just about supplier management and incident management.

**Interviewer** 14:17  
Would you say that the process of adapting your organization to new legislation such as DORA, does that process differ significantly based on organization or organization size or is it kind of the same no matter where you are?

**Interviewee 1** 14:26  
Yeah well what they are trying to do is to implement the the same legislation, no matter the size or type of your organization, right?  
So if you look at one of the first articles of Level 1 DORA, they list, I think 30 or 20 something different type of organizations. So credit unions, funds, all these other types and the last one is suppliers.

**Interviewer** 14:56  
Mm hmm.

**Interviewee 1** 14:57  
So they try to impose the same rules on all all of these companies. You can have a fund with 10 people right. And then they say in the risk management framework, you have someone towrite down the framework, someone to implement it, someone to oversee it, someone to audit it, internal audit, external audit. Basically for smaller companies that's, you know, physically not possible. You know, you have kind of conflict of interest unless you have some third parties that that can do the assessment but then it's considered external auditing in comparison to the internal audit, but overall I think one size does not fit all, so that's impossible.  
So they need to elaborate further on this proportionality. [COMPANY] are relatively small compared to all these big banks and other financial institutions, a lot of these things simply do not apply for us, right?  
So for example, they have a lot of stuff about management of your source code, let's say about testing, about having separate testing environment and not to test in production. So all of those types of things, while most of these funds such as [COMPANY] it simply does not apply to because we don't do any software development, right? And even if we do have, they are third party companies that are developing it and of course we need to make sure that they are respecting all these rules and and regulations.

**Interviewer** 16:27  
Mm hmm.

**Interviewee 1** 16:36  
But yeah know there are lots of things that don't simply. And then I actually had long discussions with your colleagues about this. Basically what I did initially when I wrote all these policies and procedures, I said, you know what, this is not applicable. So I'm not going to waste time on it, I'm just going to skip through it. And then they asked me to come back to it and everywhere where I skipped those things I needed to write down. Why did I skip it? Why is it not applicable for us? So in the end, you know we tried to make it that one size that fits all.  
You know, it's just that we had to explain why some parts of it do not applicable for us.

**Interviewer** 17:25  
Yeah.

**Interviewee 1** 17:31  
We have a lot of policies saying that even though we don't do software development, you know, we make sure if the third party is developing it for us, then they are respecting these rules and so on right, And that’s just one example there.

**Interviewer** 17:45  
OK.

**Interviewee 1** 17:47  
There are so many things that are simply not applicable for us because we don't do these things. You know, there is a lot of story about using cryptographic keys and and you know how to rotate them. And I mean that makes sense for a company like ABN where they have 1000 developers. Well, not 1000 maybe a couple of 100 developers and production system developement in their own home and they have their own data centers and hosting and all that stuff for that. I do see a need for these things, but you cannot ask the same questions for a smaller fund that has 10 employees. That's where basically the the struggle is.

**Interviewer** 18:27  
OK. Yeah, so they're kind of asking for one standardized process around, like adapting this risk management thing. And it might be feasible for larger companies, but not for smaller companies?

**Interviewee 1** 18:40  
Yeah, indeed.

**Interviewer** 18:41  
I would like to show you the pipeline I've made of the of how this goes. So it's a graphic format. It doesn't include people.

**Interviewee 1** 18:51  
Mm hmm.

**Interviewer** 18:55  
I think you can see my screen right now.

**Interviewee 1** 19:08  
Yeah, yeah, it's it's quite tiny. Even though I have it on the big screen. So maybe you can zoom in on one part of it, at least the the left side and then, yeah.

**Interviewer** 19:12  
Sure, I’ll zoom.

**Interviewee 1** 19:21  
OK.

**Interviewer** 19:22  
These are the run and change states. That's kind of what I've placed it within.  
So new legislation comes in there and then the process start and we're already going to focus on this phase.

**Interviewee 1** 19:31  
Mm hmm.

**Interviewer** 19:35  
So this part to your right is the operational execution phase.

**Interviewee 1** 19:36  
Mm hmm. Yeah, that's for later. Yeah. Operational. Yeah.

**Interviewer** 19:40  
Exactly. So we're gonna look at how new legislation comes in, how we analyze it and what we do with it. So this is the main focus. Let me walk you through the pipeline.

**Interviewee 1** 20:00  
Sure.

**Interviewer** 20:03  
The company's risk appetites defines what we can accept and what we can't.

**Interviewee 1** 20:09  
Mm hmm.

**Interviewer** 20:10  
The first step is the scoping of the new material. So reading through legislation. Seeing what it's about, the idea behind it, determining the scope, purpose and nature. Reviewing it, and from you can see which parts of these are relevant for us and which parts are not.

**Interviewee 1** 20:19  
Mm hmm.

**Interviewer** 20:26  
And why are parts not relevant especially? After that is done a gap analysis is conducted in which you check what do we already do in our current system? What do we not do yet? You identify the differences, OK?

**Interviewee 1** 20:45  
Yep.

**Interviewer** 20:49  
And from that on, we go to the control design or redesign phase in which you develop your new measures, whatever you have to do to ensure compliance with the legislation. And this could mean either updating an existing control.

**Interviewee 1** 21:02  
Yeah, or creating new controls, mm hmm.

**Interviewer** 21:02  
Yes exactly. It is per analyzed gap and then basically you do this whole thing and you get a new internal control framework.

**Interviewee 1** 21:12  
Mm hmm.

**Interviewer** 21:14  
And then it gets implemented, it goes to the second phase.

**Interviewee 1** 21:17  
Yeah, yeah, yeah, yeah.

**Interviewer** 21:17  
We're focusing on this. And throughout this whole process I have a very big column here that says communication with stakeholders.

**Interviewee 1** 21:22  
Yeah, very important indeed.  
Yeah, it's, it's actually, I mean, well done. If you came up with with this on on your own.

**Interviewer** 21:34  
Yeah, I did.

**Interviewee 1** 21:35  
Because this is exactly what we did with DORA. So I mentioned joining [COMPANY] about like 2 1/2 years ago and that's roughly the time when when DORA was announced initially, and the initial level one phase was published.

**Interviewer** 21:55  
Hmm.

**Interviewee 1** 21:55  
So what we did about it is first indeed the scoping. So basically: What is it?  
Are we in scope or are we out of scope for it? And to what extent is this going to impact us? But you know, as I mentioned, one of the first articles in DORA says that it concerns financial institution over 10 people. So basically it was already clear for us that we are in scope for DORA itself. And then what happens next is basically gap analysis. Actually a couple of them, because of how DORA was initially released.

**Interviewer** 22:22  
Uh huh.

**Interviewee 1** 22:37  
SO first level 1 and then they said, OK, we're going to go back and forth with the parties that we are going to regulate. We're going to collect their feedback. Then we're going to update it. Every six months there was a new update of DORA, right?  
So I did the initial gap analysis I think back in 2023, at the beginning of 2023, and then after that, it was basically that we identified what we would need to. We did not have let's say a defined access management policy, but it was part of the kind of operational guidelines, right? So we had to carve it out and then make links and so on. And it was the same for many other policies. However, some policies we simply did not have. And for some of them we thought, OK, let's just skip them because they are not applicable. And then after discussing it with auditors, they said even though it's not applicable for you, you have say why is it not applicable. So to go back to your second step, we did a couple of these gap analyses. So it was kind of a cycle but that has to do with the fact that we did not have the final DORA regulation. Because up to this date, you know there were still updates about it.  
So there is always this, you know, component, this gap analysis was kind of you know a cycle.

**Interviewer** 24:05  
Mm hmm.

**Interviewee 1** 24:06  
There were a couple of cycles in there and then after we identified the gaps, then indeed we went into control redesign. And actually this is something that I'm busy with at this point in time, because we are now preparing for the audit of 2025. So we usually start like mid mid year to audit the first part of the year and then somewhere in October, November we do the second part of the year and then it's one combined report. So what I'm doing now is basically making sure that our existing, what you had a bit up in in this diagram, yeah the run-state, so the risk management controls.  
So running state is basically what we had before DORA. Now we are updating the control designs.

**Interviewer** 24:59  
Uh huh.

**Interviewee 1** 25:02  
So indeed we are going to keep all our controls that are already aligned with DORA and we will create new controls if needed, or maybe some of them will be updated if we can. We will add a few new controls that are specifically related to DORA, but indeed it's per gap. So if there was a gap identified that, for example, we are missing certain policy. Let's say for example a password management policy, then there must be a control related to these policies where we say: OK periodically we export the list of users using certain password manager and we check their computers that they are not using any other password management or something like that.

**Interviewer** 25:48  
Oh.

**Interviewee 1** 25:49  
And then you watch the score from the password management application.  
And it's basically one of the these controls that we added additionally. And then again it goes to the right side, and I really like the part where you mentioned the communication with stakeholders because that needs to be happening all the time. So basically throughout all of my gap analysis I had to report to our management.  
So even to the supervisory board and different committees that are relevant for this.  
And as a result of the new policies and procedures a new framework came up out of it. I had to spend a lot of time training people about these policies and procedures. We incorporated that into our regular security awareness training where we talked about all these new policies and procedures.

**Interviewer** 26:49  
OK. And then?

**Interviewee 1** 26:49  
So this is basically the communication with stakeholders, not only employees, but also you know relevant people, because obviously you cannot just come up with with new policy and start enforcing it. It needs to be reviewed, it needs to be approved by the management and then eventually you train people only when everyone is trained, then you can start enforcing it.

**Interviewer** 27:01  
Mm hmm.

**Interviewee 1** 27:13  
But yeah, indeed. Well done on this. I think you captured it quite well.

**Interviewer** 27:18  
Nice. That's good to hear.  
And we talked about it, but throughout this whole process, what would you say are the pain points where you struggle currently and maybe even you see potential for support with artificial intelligence?

**Interviewee 1** 27:40  
Well, obviously the struggle was with redoing this gap analysis all over again. So what I did in this gap analysis, I broke down the whole regulation into each article and then say OK, is it applicable for us? Does it make sense? And did we do what the regulation says what we should do? And then if the box is green then you move on.  
But then in the next iteration, not only do you have to check the things where you had gaps identified, but also you have to recheck the whole thing, right?  
So you know, where I think the AI could help significantly is by summarizing. I mean AI is good, it's basically Learning Language Model, right? So you can give it version 1, give it version 2 and say OK summarize me the changes. And then feed that into your gap analysis. It would make much more sense to that if you did a gap analysis on one version of the text and then suddenly there are changes that you don't have to redo the whole thing. You can do the comparison with the what changed compared to the last version. And then you audit those articles. I think that that could save a lot of time.

**Interviewer** 29:21  
Mm hmm.

**Interviewee 1** 29:22  
You know the the reason why we started working on DORA two years ago is because we felt that if we wait for the final version, we won't make it in time. And that turned out to be a good decision because basically DORA kicked in in January, and then you know in April they already asked you to submit the final version of your supplier register. If you waited and did nothing, it's I think personally impossible to do it in two months. To identify all of your suppliers, the contracts, the values of the contracts, the start dates, end dates. RPO, RTO for the services which are critical, which are not. Especially, you know because again we are quite small, right? Imagine that.

**Interviewer** 30:12  
Mm hmm.

**Interviewee 1** 30:14  
Imagine how it is in a bank such as ING, you have suppliers for different branches and then you have to consolidate all together into one. It's a mess, yeah.

**Interviewer** 30:27  
Yeah.

**Interviewee 1** 30:27  
Yeah, so AI could definitely help there and what I struggle with with AI is the borders. You know, if you can have your own model and and you have your own isolated environment, then I wouldn't mind feeding all this confidential information to AI like your own control framework and have it do your gap analysis. But using the AI tool that is publicly accessible like, I don't know, chatGPT or whatever, copilot.  
I think it's asking for troubles.

**Interviewer** 31:05  
Mm hmm.

**Interviewee 1** 31:08  
You know, it's crazy to do this thing because you know it's public.  
It's learning from the text that you feed to it.  
So basically on the other end, there is someone who might be potentially malicious, users who can say, OK, what are the gaps in [COMPANY] environment and then they get basically a blueprint of how to attack [COMPANY] because they know exactly where gaps are. and so from that perspective I would be a bit hesitant to feed everything into it. But indeed it can definitely help with control redesign, and I have to say I did use AI tools at the later stage, when the Dora regulation was completely defined. But I used it in a way that I did not give it much input, at least not company related information. I actually did not share anything.  
I don't think these learning models even know what the name of the company I'm dealing with is. So I said OK, according to DORA article this and according to its document here that you can, you know, upload to to the AI tool. And according to this write me down a template of a policy.

**Interviewer** 32:27  
Mm hmm.

**Interviewee 1** 32:27  
I did not say anything about the name of the company, I did not say anything about the size of the company, but I mean obviously if it's smart enough it can read your IP address and link it to where you are registered.

**Interviewer** 32:41  
Well, yeah.

**Interviewee 1** 32:42  
But you know, I like to say that, you know, I did not put any confidential information in there.  
But if I did not feed our current control framework into it, so it could help it with the Step 3 here as well, right?

**Interviewer** 32:50  
Mm hmm.

**Interviewee 1** 32:59  
So you, you know, once you know what your gaps are and once you close your gap, you could feed entire framework into the AI saying OK, this is my framework.  
Help me define the controls and this is my old framework so I need you to define new controls. I'm pretty sure if I would have that freedom to upload all of our information to it I could probably use it, you know and and it could help a lot.

**Interviewer** 33:22  
Mm hmm.

**Interviewee 1** 33:26  
But again, there is this aspect of, you know, data confidentiality, because I simply don't trust these tools enough to feed all this confidential information to.

**Interviewer** 33:37  
Yeah. Yeah. That that does make sense.  
And so yeah, you mention data confidentiality, privacy and other aspects. Are there other aspects around AI that are important or interesting to you? Because I mean, as you might be aware, those models really boil down to statistics, determining like what is the most logical next letter.

**Interviewee 1** 33:44  
Mm.  
Mm hmm.

**Interviewer** 33:57  
It doesn't have an actual understanding.

**Interviewee 1** 33:58  
Mm hmm mm hmm.

**Interviewer** 34:02  
How do you think that plays a role in this. Let's say you were to use AI what do you think about the output.

**Interviewee 1** 34:12  
I mean on one hand it doesn't fully understand, but I don't know if that's a good or bad thing, to be honest, because if it doesn't understand, then it also does not understand what are the risks related to publishing that kind of information. For them it’s just a bunch of text but for others you know for potential malicious people or even competitors or whoever you know wants to deal damage to your company, it can contain very valuable information right? And and the other thing is that all of this data that you upload to it, it's basically your data that you deliberately shared with third parties that you don't know. In the end you do know who owns the company and who owns the servers and all that, but it's not gonna forget this data in one year and, three years or even five years from now, right?  
So we have to be careful that even though maybe it's not understanding, you know it's not a human being behind this whole thing, but eventually these things will evolve and your data will still be there.  
It might not be 100% up to date in three years from now, but why would I give my you know the the you know if if we are talking about

let's say different tools that we are using, tools for project management tools for  
Password management tools for basically day-to-day operations. If you are using Microsoft or Google, some of these things might have certain vulnerabilities in an upcoming period that that could allow people to get inside of our organization. And if you go further, if you're providing evidence that you’re doing these controls, then it can go into even usernames and things like that.  
So yeah, maybe it's not that smart at the moment, but it will certainly keep all of the data that you feed into it and maybe some models with with computing and something that that's just around the corner.  
You’re just giving a lot of information for free and unnecessary.  
Yeah, maybe you will save couple of hours of work. But overall I think, and that's my personal point of view here, I don't think at this point in time it's sufficiently tested.

**Interviewer** 36:26  
Mm hmm.

**Interviewee 1** 36:39  
And it can’t be trusted.  
Unless you can, let's say use it from your own isolated environment.  
Put your own computing resources and everything else in your whatever server room and then feed into that and let it play around with that.  
For that part I could maybe discuss it, but after that you you really wipe out those servers and and nothing is left on on that maybe that would be an option for me. But to feed it into some public AI tools? I don't think so.

**Interviewer** 37:12  
And then let's say you do have, like, your own offline trained model AI tool.  
To what degree do you think you could? You would use it?  
Would it be an independent running program?  
Would you use it as a tool ? How would integration be with your current process?

**Interviewee 1** 37:33  
Well, definitely if it could be isolated. If someone would in theory tell me, hey, nobody else will ever read this data and I could guarantee that myself then why not, you know? Let's see what it can do like and then I would be open, to test it at at full potential. But until that happens, yeah, I'm. I'm a bit hesitant still, yeah.

**Interviewer** 37:56  
Of course, and. And what would be the full potential you think then?  
So let's say it is possible to get it fully privacy secured.

**Interviewee 1** 38:05  
Yeah, but then then a lot of these things could be automated.  
You know, OK.  
Hey this is a new regulation.  
This is what we are doing about it.  
You know, do me scoping, you know, is it applicable for me or not?  
Yes, no, fine. OK.  
Yes, do the gap analysis.  
You know, this is what we do.  
You know, feed in with with your current framework.  
You know what? Whatever is it that your, your policies, your procedures, your evidence.  
And then propose how we can redesign our controls.  
You know that's all there is and maybe even go one step further.  
How many of these controls can we automate?  
Let's say one of our controls is is comparing the asset management inventory, let's say just we link that to our Microsoft environment. You know, take all of the list of assets, compare it with our own inventory.  
You know is there are there any mismatches and what can you do to to help us mitigate those?  
Or or to resolve these. You know, I I think the the possibilities are limitless here. If you could guarantee that you know it would simplify a lot of and it would replace a lot of manual work I think.

**Interviewer** 39:22  
And where do you think the accountability would lie?

**Interviewee 1** 39:28  
Well I think very important component here is to still have human control.  
In a driving seat here that verified that you know whatever this thing spits out that that it kind of makes sense right. I think it's not that good yet.  
It's not at that level of development yet that it can do these things on its own, but maybe in in couple of years it will be better. But you know obviously you cannot give accountability to an IT system. So as far as my knowledge goes, you know, so you cannot blame the the system if it did something.

**Interviewer** 40:13  
Hmm.

**Interviewee 1** 40:20  
Even though we we sometimes try to do that, there must be someone who is in charge and that this does not replace basically the governance part that also was defined indoor and all the other Reg.  
So you must have team who is checking it.  
Who is auditing it?  
Who is making sure that the controls that you say that you do, that you actually do them, but also on let's say auditing side, it can be if you could have your own environment and you say OK: We are auditing [COMPANY] on DORA, give me evidence of all these policies and procedures, you pack them in in one zip file, you put it into AI tool and then identify the gaps.

**Interviewer** 41:08  
Mm hmm.

**Interviewee 1** 41:10  
Right. So it it would simplify a lot of process that currently [PEOPLE] were doing manually.

**Interviewer** 41:18  
Mm hmm.

**Interviewee 1** 41:26  
Yeah, I think it it could be automated a lot.

**Interviewer** 41:37

But you said the humans remains in a driver's seat, so AI would ride along with it? It would never be in in full control and taking accountability?

**Interviewee 1** 41:40  
Yeah.  
Yeah. And until it becomes a person that can be responsible for it, yeah, it's it must be a human behind it.

**Interviewer** 41:56  
OK.

So let's say in an ideal future we develop a tool like this, if you could make a list of the three main or most valuable features of such a tool, how would you rank it? Like where do you see the most potential and where maybe not so much?

**Interviewee 1** 42:25  
Well I mean you can probably link it to those three things that you mentioned, I mean obviously the scoping part is not that complicated you know either you are in scope or you're not right. So but you know there is always some gray area.  
Sometimes it's not clearly defined so maybe it it could help on on that part.  
But definitely I would put the highest priority with the gap analysis, because that would determine also the input on the next stage or the control redesign. Because once you identify the gaps, it is pretty straightforward what you need to do with your controls.  
So let's say maybe the the the first part is the least important. I would focus that the gap is gap analysis is the first one, control design 2nd and then the scoping part as the third one.

**Interviewer** 43:32  
Ok, thanks. And are there then any systems that you think AI would integrate with currently? Or would it be like a program you just fire up?  
Is that even relevant to you?

**Interviewee 1** 44:07  
Yeah, I think it would be useful to have these all these things in one system where you can prove to the auditors, OK, we have these controls and all that stuff.

But that that part can even be in a simple excel sheet where you say OK.  
These are these controls and and this is where we store the evidence, right?  
What I would like to see instead is to help us maintain all these controls and maybe link it to let's say software like project management tools like Trello or [INAUDIBLE] or something like that where it gives you a dashboard with the controls.  
And then, you know if it could automate some of these things, you know, if we need to export, let's say, a list of users, a list of devices for asset management, a list of whatever on a periodic basis, that it can do that part automatically as well.  
So you could link it to your Microsoft 365 environment. You could link it to to your local network. Let's say if you if you are talking about you know network monitoring and things like that.  
So it could be basically a very informed additional hands for maybe the head of IT department or IT manager or however you want to call it. It could be linked to your mail system. So it throws you an alert saying hey,you had an IT incident that needs to be reported and stuff like that so.  
Yeah, I would link it to many other systems, not just for the framework itself.

**Interviewer** 45:36  
Mm hmm.  
OK.  
All right.  
Well, that's that's good to hear.  
So basically within this interview, you recognize the pipeline as being accurate at least, so that's good.

**Interviewee 1** 45:56  
Yeah, definitely.  
Yeah, yeah.

**Interviewer** 45:58  
You see a lot of potential for AI in the gap analysis. So that's good to verify.  
But for everything to work out the very fundamental thing for you is the privacy aspect and the data security.  
You think none of this would work if you can't guarantee the data privacy.

**Interviewee 1** 46:14  
Yep, Yep, indeed.  
Yeah, I mean, I wouldn't say none of it would work because the AI tool still did a lot of work for us when it comes to, let's say reading this framework and you know all these policies and procedures. But as I mentioned to you, I said OK, give me an example of policy aligned with this DORA article and its RTS document. And propose me a policy and or related procedure about that.  
So at least I'm sure that it will mention all of these things that need to be mentioned because that's basically, you know, that's what current tools are good at.

**Interviewer** 46:50  
Mm hmm.

**Interviewee 1** 46:59  
But then I still have to go through it and this is where I said, you know, this human factor needs to be in there.  
So I went through the proposal document, I filtered out the things that are indeed applicable, that are acceptable for us. Some things I had to change to describe how they are currently because it sometimes struggles. You know in an ideal world you can define how something should work, but you could.  
You should actually define how is it that you are doing the things that you promised that you're doing.  
The end result was, you know I got the general template.  
Let's put it like that where it says, you know, fill in your company name here and fill in this and that.

**Interviewer** 47:36  
Huh.

**Interviewee 1** 47:40  
And then the policies like it's 80% done. You know once you get it from the AI tool, even with this current technology and then you just have to adjust it to to fit your needs.

**Interviewer** 47:48  
Mm hmm.

**Interviewee 1** 47:54  
And obviously, to make sure that it makes sense to your own company.  
So you have to tailor it, but you know, but you know, in ideal world it it could be that it does 100% of it, but in order to be accurate and complete you need to give it a lot of information and at this point in time I'm not ready to give all of this information.

**Interviewer** 48:17  
Yeah, but for you believe it can take away a lot of manual labor.

**Interviewee 1** 48:23  
Yeah, because yeah, imagine that you have to read like DORA itself is probably more than 500 pages, right? I mean I did read good part of it where I thought it would be necessary and where it would make sense. But you know it's impossible for a single human to have all all these aspects in their head.  
You have to have this policy, that should contain this, this and this and this, and by the half of reading all these articles you're already lost.

**Interviewer** 49:00  
Mm hmm.

**Interviewee 1** 49:01  
While you can ask AI tool hey, write me down the policy according to this article and and this document and then it will certainly not skip any of these parts later on. It goes through everything.

Imagine if you have to write down these policies by yourself. I don't think it's possible. Well, I mean it is possible, but it would take you ages and a team of 50 people like it happened with one of these banks.

**Interviewer** 49:28  
Mm hmm.  
So what I'm kind of getting at is, is.  
The main issue throughout this whole thing or pain point is that it's just there's a very large documents that you have to read not even once, but maybe a couple of times.

**Interviewee 1** 49:45  
Yeah, indeed.

**Interviewer** 49:46  
That's kind of what it's about.

**Interviewee 1** 49:46  
Yeah, man, it saves you a lot of time and it can summarize you quite accurately what needs to be done.

**Interviewer** 49:53  
So summarization, you're probably quite experienced with AI, so you know what Large Language Models are?

**Interviewee 1** 50:03  
So it's LLM. So it's learning.

**Interviewer** 50:07  
They're trained on language

**Interviewee 1** 50:10  
So the more information you give to it, the smarter and better output will be of course.  
But yeah, that that's what it's good with.

**Interviewer** 50:17  
Mm hmm.

**Interviewee 1** 50:19  
So yeah, we should use it, you know? But we should be careful what we put into it, yeah.

**Interviewer** 50:24  
Yeah.  
Are there any challenges you faced throughout this process? Or have we kind of grabbed it all here?

**Interviewee 1** 50:44  
Yeah, I think we we we grabbed everything already.

**Interviewer** 50:50  
OK.

**Interviewee 1** 50:52  
Yeah.

**Interviewer** 50:52  
OK. That's then I guess about it.

**Interviewee 1** 51:26  
Yeah, indeed.   
So for me, I I would be willing to experiment with it if someone could guarantee or if I could have the capacity and time to build my own sort of server room where you can, you know, train your own models and play around with it With some assurance that the data that you put in there will never leave it.

**Interviewer** 51:50  
Mm hmm.

**Interviewee 1** 51:57  
But yeah with these public tools, I don't think it's a good idea.

**Interviewer** 52:02  
OK.  
Perfect. Well, that is everything I have for today. You've really helped me out here.

**Interviewee 1** 52:15  
Sure. Yep, of course.  
Yeah, well done on this part of identifying those three steps because that's exactly what we saw in practice.

 **Interviewer** stopped transcription