Opening Statement

Interviewer:
Good morning and welcome. First of all, thank you very much for your willingness to participate in this interview. My name is Imane Akhyar and I am a master's student in Information Studies at the University of Amsterdam. This interview is part of my thesis research at [Company Name]. The research focuses on how to effectively integrate artificial intelligence into the cybersecurity risk management within financial institutions.

The talk will last about 60 minutes but I think we will be done after only 30 minutes. All answers will be completely anonymized and kept strictly confidential. You are of course free to skip a question or end the interview at any time.

Do you have any questions at this time before we get started?

Respondent:
No, everything is pretty clear.

Section 1: Background of the interviewee

Interviewer:

Before I continue, I would like to briefly explain that the interview has two parts, the introduction questions and the key questions. First, I will start with the introduction questions:

Q1.1: Can you briefly tell us something about yourself and your role within the organization?

Respondent

My name is [Name] and I have been working as a director within [Name of Company] since January. Within our organization, I am specifically responsible for serving clients in the financial sector, specifically banks. Before taking on this role, I worked as an auditor, where I gained extensive experience in the areas of supervision, auditing and risk assessment. This background now helps me to properly advise clients on governance and risk issues, especially in relation to new technologies such as artificial intelligence. And recently I also belong to the firm's AI group.

Interviewer:
Q1.2: How much experience do you have with cybersecurity, risk management or AI?

Respondent:

I have nearly a decade of experience as an IT auditor, with a focus on technology risks within various organizations. From that role, I have been heavily involved in cybersecurity and risk management in a broad sense. Although AI was not central to that until recently, I see that it is now becoming increasingly relevant. That is why I have now joined an
AI working group within our organization, in which we examine how to apply AI responsibly and effectively. That combination of background in technology and risk management helps me get a good overview of the risks and opportunities of AI. I also supervised a number of theses on AI and risk management last year.

Interviewer:**:**
Q1.3 To what extent are you familiar with LLMs or other AI technologies in your work context?

Respondent:
I mainly have experience with ChatGPT and see that it is also widely used within our organization and with customers.I also hear positive stories about other models, such as Claude. We are still in an exploratory phase, but I see a lot of experimentation and collaboration with existing tools. However, there remains a certain reluctance: I often ask myself how reliable the output is, and whether the input data has been sufficiently verified. Those kinds of questions are coming up more and more, especially in critical applications.

Interviewer:**:**
And lastly:
Q1.4 Are you familiar with regulations such as DORA or the AI Act?

Respondent:
Yes, I am familiar with the GDPR and the AI Act, and see that they are increasingly impacting how organizations deploy AI. There is a lot of overlap between different regulations, which makes it important to live through this carefully when creating internal policies. For example: is something allowed under the AI Act or not allowed? These are considerations you need to make early on. In our organization, I see that proportionality is an important principle. We are not a big tech player, but we do want to be able to justify responsibly how we use AI. That is why we sometimes involve external legal experts to check whether our use fits within the legal frameworks

Section 2: Thematic depth

Interviewer:
Well great those were the introduction questions. The next questions are about components of the framework. These are more substantive questions about the topics and the last two questions are about the preliminary framework.
Q2.1: At what points within cybersecurity and risk management can
Do AI models provide the most value? And specifically I am talking about the financial sector.

Respondent:
I think that especially in processing very large data sets, there are a lot of gains to be made so that you get better insight and don't have to do everything yourself. I think if you deploy it in the right and safe way, it saves manpower and can provide a lot more insight. With the caveat, though, that there is also more and more data coming in, and it may be difficult to always have full insight. I actually think that may not be possible at all, but I do think it helps a lot in that regard. In risk management, I think that setting up processes more efficiently and automating them, for example having all reports go automatically, can be very helpful. Coincidentally, last week we had a customer with a very nice dashboard for management information, from all kinds of fancy PowerBIDs. I then asked, "What is the source and is it complete?" There was really no answer to that at all. Then you run into it: where does the data come from and how do we know if the data is correct?

Interviewer:
So another thing that comes out of this is that the source of the data plays a big role in this.
Q2.2: Are there certain AI tools that you think are very useful, for example ChatGPT?
I actually have mostly experience with ChatGPT and I see it around me the most. Other than that, I haven't used many other AI tools. I do hear good stories about the paid version and think it could also be very useful within the organization itself. If we were to use it here, we work in a Microsoft environment , then CoPilot will be fine as well. But I am still somewhat hesitant about whether everything is correct. I really ask myself a lot of questions. I sometimes think: how do we know this for sure? And if someone inputs something and an answer comes out, how can we be sure that that answer is correct.

Interviewer:
In previous interviews, the greatic of monitoring the use of AI systems came up frequently. Some organizations already have explicit policies in place for this, while others mainly emphasize the importance of logical thinking and common sense in their use.

Q2.2: How is AI systems overseen in your organization?

Respondent:
Right now we are still building our governance around AI. While there is already a broader Society & Security policy within the organization, we are finding that AI requires its own approach. Therefore, we are in the process of creating a separate AI policy, separate from that existing framework.

We think it is important that employees are actively included in that policy, so that it is not just a document on SharePoint that no one reads. For us, supervision should not only be formal, but also supported in practice. That's why we involve different disciplines in drafting it and also look at how we can increase knowledge sharing and awareness about AI. It's really still in development, but serious work is being done.

Interviewer:

Clear, thank you. So you indicated that the monitoring of AI is still in development and a separate AI policy is being worked on. An important aspect of this, of course, is the role of laws and regulations.

Q2.3: How do GDPR, DORA, NIS2 or the AI Act affect the use of LLMs in your organization?

Respondent:
Yes, obviously there is some overlap between those different regulations. That's why it's so important to go through them properly before you get started with AI. If you're drafting a policy, you really need to check beforehand: is this allowed under GDPR? And what about the AI Act? I did a project last year that addressed that as well, and it showed that proportionality is a very important principle. The same applies here with us. Of course we are not a big player like Microsoft, but we do want to be able to explain responsibly why we do something, and how we record it. We want to be able to look back with a good feeling that we set this up with care and awareness.

It does require cooperation. It is not something you just think up or impose on your own. It really is a joint responsibility to make policy that fits both the regulations and our organization. That is still a challenge, but one we are actively working on.

Interviewer:

I also have some questions about ethics and privacy. These are of course two terms that come up quite often in the use of AI.

Q2.4: What ethical risks do you see with the use of LLMs?

Respondent:
There are certainly ethical risks. A major issue is the quality and origin of the data used to train LLMs, there is not always transparency about that. You sometimes

not exactly what a model is based on, and that makes it difficult to properly assess the reliability of the outcomes.

In addition, I see the risk of people becoming too dependent on AI. There is a danger that, as a user, you lose your own critical thinking skills and just blindly adopt what a model returns. Whereas you should actually keep thinking: is this right? Do I understand what this says? Especially when it comes to complex or policy-based information, this is crucial.

What I also notice in practice is that there are increasing concerns among employees about the use of AI, for example that some or all of their work will be taken over. This fear is also prevalent in LLM applications. It raises questions about job security, role changes and future-proofing of functions. These are themes that, as an organization, you must also pay attention to, and include in your ethical considerations.

Interviewer:

And often organizations want to take advantage of the speed and efficiency of AI, but at the same time maintain control over what happens to it.

Q2.4a: In your opinion, is human control always necessary, or can certain decisions also be fully automated?

Respondent:
I believe that some form of human control is always needed, especially with important or sensitive output such as policy documents, reports or opinions. For simple tasks such as translations, for example, you might be fine to let AI do something independently, but as soon as it becomes substantive or strategic, someone really needs to be watching.You can use AI as a tool, but it should never take over final responsibility. People need to understand what was generated and be willing to correct or adjust that as needed. In the end, we deliver something to the customer, and then you have to be sure that everything is correct. So there should always be a final check, so you can stand behind the quality of the work with confidence.

Interviewer:
You mention several times how important the provenance and reliability of data is. **Q2.5: In your opinion, how important is data quality and control in AI applications such as LLMs?**

Respondent:
This is incredibly important. The input data has to meet certain conditions before you can use it responsibly in AI applications. If you don't know where the data comes from, or how it was created, then it becomes very difficult to trust the outcomes. Especially with models that generate large amounts of text or information, it's crucial to understand the basis on which the model bases its predictions or output. At the same time, you also have to be realistic about that. You cannot fully vet or manually check every dataset, especially if you are working with limited resources. That's why it's important to take a proportional approach: you have to be critical, but also remain workable. It's all about awareness, clear ground rules and good risk management when using data in an AI context.

Interviewer: Besides the data, it is also important that the LLMs are used in the right way, within the company.

Q2.6: How is it controlled how LLMs are deployed or modified?

Respondent:
We are still in the early stages of developing controls around the use of LLMs, but what we are already doing is putting a strong focus on education and awareness. Within our organization we have a user group where people share experiences, ask questions and discuss risks. That knowledge sharing is incredibly valuable.

In addition, we regularly organize internal knowledge sessions to make colleagues aware of both the opportunities and risks of AI. Not everyone has a technical background, so it's important that people understand exactly what an LLM does, what to look out for when using it, and how to handle inputs and outputs responsibly. We believe that well-informed employees are ultimately the best first layer of control. So instead of plugging everything in with technical restrictions, we now emphasize training, open dialogue and shared learning opportunities. That forms the basis of our approach.

Interviewer: So those were the substantive questions. The next two questions are about the preliminary framework.

Q2.7: What do you think is needed to have confidence in an AI-supported framework for cybersecurity risk management?

Respondent:
To have confidence in an AI framework, it is important to be clear where it starts. Do you start with policy or just technical risk analysis? That order determines how the parts fit together logically. If that is unclear, it becomes difficult to apply the framework properly.

In addition, what I find essential is a clear link with risk assessment. You first have to know which risks are relevant in your context before you can determine appropriate measures. I still miss that step; without that analysis, you quickly end up with generic controls that do not always fit the practice.

The framework must also be flexible enough to be applied within different types of organizations, which works for a large bank, not necessarily for a smaller party. And finally, review. It should name how it is validated, by whom and based on what criteria. Only then will the framework remain current and useful.

Q2.8: Which parts of the framework do you find most relevant or problematic? Are you missing certain elements or do you see opportunities for improvement?

Respondent:
What I found very strong about the framework is that it touches on several relevant topics, such as data, lifecycle, governance and ethics. But there are also elements that I think could be further strengthened. One important one is education. In practice, I see that knowledge about AI is very unevenly distributed within organizations. Some employees are

digitally proficient and experiment in abundance, while others hardly know what an LLM actually does. If you then develop a framework that must contribute to the responsible implementation of AI, it must contain a clear educational component. Not just one-time training sessions, but structurally: onboarding, repeat sessions and accessible documentation. AI literacy should really become a basic requirement.

In addition, I miss attention to knowledge sharing as a structural component. AI develops rapidly, and organizations learn a lot by doing. It would be nice if the framework encouraged active sharing of experiences, successes and mistakes, within teams, between departments, or even across organizations. That way you build collective intelligence and prevent everyone from having to reinvent the wheel. And finally, I would suggest making an explicit distinction between the 'run' side and the 'change' side of AI deployment. So on the one hand the daily use (run) and on the other hand the change, innovation or implementation (change). The two require different forms of governance, risk assessment and human involvement. By including that distinction in the framework, it better aligns with how organizations actually work.

Interviewer:

You made some valuable points, such as the importance of a clear start and link to risk assessment, as well as the need for flexibility and testability. Education also came up in the previous interviews, so I will certainly incorporate that into the framework.

This brings us to the end of the interview. As mentioned, I am going to incorporate the results from this interview into the further development of the AI framework. Based on all the interviews, a modified version will follow, which I will share with you via a short Google survey in the second week of June. That will contain five to six simple, closed-ended questions to validate the framework, and will feature a clear deadline at the end of the same week.

Thanks again for your time and valuable insights, it really helped me a lot! As previously stated, all responses will be completely anonymized and used solely for my thesis. Upon completion, the data will be deleted and not used for anything else.