Opening Statement

Interviewer:
Good morning. First of all, I would like to thank you for being willing to participate in the interview. My name is Imane, I am currently doing my master's degree at the University of Amsterdam in Information Studies. This interview is part of my thesis research at [Company Name]. The research is about how artificial intelligence can be effectively integrated into the cybersecurity risk management, especially at financial institutions. The interview will last about 60 minutes. Everything is processed anonymously and only a transcript is made, which is then deleted.

The interview has two parts. First is a brief introduction of about 5 minutes and then I go to the key questions.

Respondent:
Yes, sounds good

Interviewer:
I had also sent an email yesterday with the framework, I don't know if you had already seen it?

Respondent:
Yes, I've seen it, but haven't gone through it fully yet.

Interviewer:
That doesn't matter, we won't go into too much detail. Because the questions are combinations of different elements from the framework. So the questions I ask here will eventually be incorporated into the framework. Are there any further questions?

Respondent:
And yes, and I was still curious as to why you chose the company.

Interviewer:
[Name of company] was part of the thesis market at the UvA and so they had a topic on AI how to best use it in risk management. They had still left it very broad so that the students could then come up with their own idea. Well, I had done my bachelor's at the VU and my bachelor's is AI and so this topic did attract me.

Respondent:
And what other people do you interview?

Interviewer:
I interview people from cybersecurity, risk management, governance and related fields. That way I get different perspectives. Two of the interviewees are internal to [Company Name], the rest are external.

Respondent:
Okay yes, clear.

Section 1: Background of the interviewee

Interviewer:
Well then I'm going to ask the first introduction question:

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

Respondent:
Yes no, definitely my name is [NAME]. Well, I did the same master's. I also did the bachelor of information science at the University of Amsterdam.
First my working life started in public policy around the Internet and Internet governance and later I got myself into AI risk management. And I am
I am currently on a team at [NAME COMPANY] where I have been working for 3.5 years now.

Interviewer:
What is important about your role for AI and risk management?

Respondent:
We have a diverse client base, from governments to corporations. We advise them on responsible use of AI.

Interviewer:

Q1.3: To what extent are you familiar with LLMs or other AI technologies?

Respondent:
Well, I am very familiar with that, because we advise our clients on the responsible use of it. Yes, I do think I know more than average about AI. But I don't know much about LLMs specifically.

Interviewer:

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

Respondent:
Of DORA I have been acquainted, but not substantively. The AI Act I know well and we also use with clients.

Section 2: Thematic deepening

Interviewer:
Q2.1 :At what points in the cybersecurity risk management process do you see the greatest potential for AI, particularly large language models (LLMs), to add value within financial institutions?

Respondent:

So, that's quite a mouthful haha. If I break down your question, it's about using LLMs in identifying risk at financial institutions.

Interviewer:

Yes that's right

Respondent:

I find it difficult, I have no idea. I can't answer this question at the moment.

Interviewer:

No problem!

FQ2.1: Are there any particular challenges or barriers to adopting AI solutions for cybersecurity and risk management that you have experienced yourself or seen in others?

Respondent:

A major risk is lack of education. Many people are using AI without the proper knowledge. I think the danger now is a lack of critical thinking.
There are also problems such as bias in training data and lack of transparency. What we see is that the data that is trained on is often not enough to take out the biggest piece of bias. Synthetic data can also introduce new forms of bias, particularly how it was created. And I think we're going to keep those for a while, too, because we're generating more and more synthetic data.

Interviewer:

Okay, so actually, what I take from this is that education is especially an important role, but it's also a risk because people just don't have enough knowledge of that and then bias and transparency in AI.

Respondent:

Yes, that's right.

Interviewer:

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

Respondent:

Within our organization, we work in multidisciplinary teams consisting of technical experts, legal experts and consultants. We often act as connecting link between these disciplines. From that position, we advise clients on the responsible use of AI and indicate which applications are or are not appropriate within their context. Although there is no formal oversight mechanism yet, oversight arises implicitly through this collaboration and alignment.

Interviewer:

FQ1.2: Do you experience resistance to that collaboration?

Respondent:

No, rather we see AI being applied too quickly. On the contrary, we advise clients restraint and alternative solutions whenever possible. Often they think that their way of working is right and we then discuss that with the team before a final decision is made.

Interviewer:

My next question is about regulations:

Q2.3: How do regulations such as GDPR, DORA, NIS2 or the AI Act affect the application of LLMs in cybersecurity?

Respondent:

Our clients obviously want to comply with laws and regulations such as the AI Act, GDPR and DORA. These regulations directly impact how organizations deal with AI, especially in the areas of transparency, risk classification and responsible data use. We support clients in this in several ways: by providing education sessions, conducting model reviews, and helping to classify AI systems based on risk levels. In addition, we advise on what documentation, policies and controls are required to be demonstrably compliant. In this sense, we are actively involved in translating abstract regulations into workable guidelines and processes that fit the client's organizational context.

Interviewer:

And then I have questions about the ethical and privacy concerns.

Well you had just talked a little bit about the bias and fairness points,

Q2.4: Are there any other ethical and privacy concerns with AI-driven cybersecurity solutions and how do you think they should be addressed to ensure trust and transparency?

Respondent:

Which ones exactly I can't think of right now but what you often see is the lack of understanding of metrics. So that a party is very convincing that the applications that what they are using is correct. Hence then I think the importance of frequent review processes is necessary.

Interviewer:

And what exactly do you mean by that? The review processes?

Respondent:

I would have a review take place at each step so that you can be sure that what you are using is deployed correctly. In other words, a kind of four-eye principle: AI can provide or analyze something, but there should almost always be a second check before anything is actually deployed. Especially in sensitive applications in cybersecurity, this is essential to avoid mistakes or wrong assumptions. It's about not following AI blindly, but consciously building checks on it.

Interviewer:

Okay, because that was also my next question right away:

Q2.4a: Do you think human control is always needed, or can certain decisions be fully automated?

Respondent:

I think there needs to be a risk assessment, which ones specifically do you let AI do and which ones don't, that's still a gray area. AI decision-making must always retain human oversight. Some decisions are even prohibited in certain contexts.

Interviewer:

FQ1.5a: And are there any particular tasks that you would never automate?

Respondent:

Certain tasks, such as legal decisions, should never be made by AI. At most, AI can make suggestions with accompanying probabilities.

*Interviewer***:**

Lastly, I had a question about data entry.

Q2.5: How important do you consider the quality, provenance and control of the data used in AI applications such as LLMs? And what approach does your organization take in this?

You had mentioned earlier that synthetic data can introduce new forms of bias.

*Respondent***:**

Yes, that's right. Data quality plays a hugely important role, especially in AI applications. What we often see is that while organizations want to work with AI, they don't have sufficient visibility into where the data used comes from or how it's compiled. This applies to both real datasets and synthetically generated data. Especially with LLMs, this is a risk because your model then learns something based on potentially flawed assumptions or poor representation. We try to to overcome this as much as possible by indicating to clients that you should never really just feed a model with unscreened data. There must first be a step beforehand: what kind of data is this, how was it collected, and what is not in it? Ideally, you would also classify that input data by quality or reliability. In practice, we don't always do that in a structured way yet, but we consciously discuss it in every project where AI plays a role. You also notice that many companies use models trained on open datasets or public sources, and there is little transparency in that. We also try to make that discussable - for example, that synthetic data seems like a solution, but can also create new biases.

Interviewer:

So if I understand correctly, data quality is increasingly becoming a topic of conversation, but there is no set approach or standard yet?

Respondent:

Exactly. The awareness is there, and we take it into consideration, but I think it still needs to be further embedded in processes and policies. Especially if AI is going to be deployed more broadly, that part needs to be arranged structurally.

Interviewer:

Those were the key questions of this interview. Now I would like to ask you a few more questions about the preliminary framework I sent along.

Q2.7: What would you need to have confidence in an AI-supported framework for cybersecurity risk management? And how would such a framework ideally be tested or improved in practice?

Respondent:

Within our organization, we have developed our own framework that we use in our AI and risk consulting projects. I can share that with you if necessary. What strikes me is that there are some elements similar to your proposal, which is positive. At the same time, I also see some elements that I miss. For example, I think the aspect of explainability should be included more explicitly. There is also a lack of attention to sustainability, for example in the sense of long-term effects of AI systems or the energy consumption of certain models. In my opinion, these are important additions to make the framework stronger and more future-proof.

Interviewer:

Ooh great thank you! And then I had a question about my preliminary framework.

Q2.8: Looking at the framework as a whole, which parts do you find most relevant in your practice?

Respondent:
I found the most relevant was the focus on risk classification and governance, which are topics that come up all the time in our day-to-day practice. Those components align well with how we currently approach AI and risk management within organizations. They form the core of a workable framework as far as I'm concerned.

Closing

Interviewer:

This also brings us right to the end of the interview and again, thank you for that time and your answers. And as mentioned before, everything is anonymized and kept confidential. I will only use it in the transcript for the sentences and incorporate it into the thesis. And after the thesis, everything will be deleted.

Are there any other questions or comments?

Respondent:

No further no questions

Imane Akhyar:

And after processing the results of the interviews, I send another Google Survey to all the interview candidates. This also immediately contains the final framework and questions about whether it matches what was discussed today. That way I can validate right away with everyone. You can then expect those approximately the second week of June.

Respondent:

Great! Good luck with the interviews and writing your thesis!