Section	Question or statement ID	Question or statement.	Purpose	Potential follow-up questions ID	Potential follow-up questions	Timestamp
Introduction	O.S.	x	Briefly introducing myself to the interviewee, how long this interview will take place, and the purpose of this interview.			~ 5 minutes
1) Interviewee Background						~10 minutes
	Q1.1	Can you briefly introduce yourself?	Establish name, background, and general context.			
	Q1.2	Where do you currently work, and what is your role there?	Understand their organizational setting and position.			
	Q1.3	How many years of experience do you have in cybersecurity, risk management, or AI-related fields?	Gauge seniority and domain expertise.			
	Q1.4	How familiar are you with AI technologies or applications in your daily work?	Assess technical familiarity, which may influence their views.			
	Q1.5	Are you familiar with regulations like DORA, GDPR, or the AI Act in your professional context?	Understand regulatory awareness. Crucial for framework.			
2) Core Interview Questions: Thematic Deep Dive						~40 minutes
Strategic Perspective on AI Adoption	Q2.1	From your perspective, at which points in the cybersecurity risk management process do you see the greatest potential for AI, especially large language models (LLMs), to create added value within financial institutions?	To explore the interviewee's strategic view of AI's potential applications in cybersecurity.	FQ1.1	Could you give a concrete example?	
Implementation Challenges & Organizational Readiness	Q2.2	What do you consider the biggest challenges or barriers (technical, organizational, or cultural) to adopting AI-based solutions for cybersecurity risk management in your institution?	Identify practical and cultural barriers to AI adoption.	FQ1.2	Have you experienced resistance to AI from certain departments?	

	Q2.2a	How do you see the collaboration between your department and others within your organization in relation to AI implementation? To what extent does this influence the effectiveness of AI in cybersecurity risk management?	To gain insight into organizational dynamics surrounding AI			
				FQ1.2.2	Are these challenges changing over time?	
Regulatory Compliance & Governance	Q2.3	How do evolving regulations (e.g., DORA, NIS2, GDPR) shape your organization's approach to implementing AI in cybersecurity? Are there specific compliance or governance pain points you've encountered?	Understand how regulatory frameworks impact AI implementation strategies.	FQ1.3	Are compliance teams involved in AI system development or review? If so, do they update the team about certain changes?	
Ethical & Data Privacy Considerations	Q2.4	In your view, what ethical or data-privacy concerns arise with AI-driven cybersecurity solutions, and how should they be addressed to maintain trust and transparency?	Elicit views on AI ethics, fairness, and data governance.	FQ1.4	How do you balance automation with fairness or accountability ?	
Human Expertise & AI Collaboration	Q2.5	Where do you see the balance between automated AI-driven decisions and human oversight in cybersecurity risk management? What kinds of checks or validations do you find most necessary?	Investigate the human-AI interaction and oversight mechanisms.	FQ1.5	Can you describe a situation where human review was critical?	
				FQ1.5.1	Are there specific tasks you'd never automate?	
Framework Validation & Future Outlook	Q2.6	What elements or criteria would give you confidence in an AI-supported cybersecurity risk management framework? How do you suggest it should be validated or updated over time?	Gather expert insight on framework quality, evaluation, and adaptability.			
Feedback on	Q2.7	Having reviewed the	Direct feedback to refine	FQ1.7	Which part felt	

Preliminary Framework Components		preliminary AI-driven cybersecurity risk management framework, which components do you find most relevant or potentially problematic in your context? Are there any missing elements or areas that require further refinement to improve its practical applicability?	your conceptual framework.		most realistic or unrealistic to you?	
Closing section of interview questions		Closing statement				~ 5 minutes

Opening statement:
Thank you for agreeing to participate in this interview. My name is Imane Akhyar, and I'm a Master's student in Information Studies at the University of Amsterdam. This interview is part of my thesis research, which I am doing at Kouters van der Meer, on how artificial intelligence can be effectively integrated into cybersecurity risk management within financial institutions.

The interview will take approximately 60 minutes and will be recorded for research purposes. Your answers will be anonymous, and you can skip any question or stop the interview at any time.

Do you have any questions before we begin?

Closing statement:
That brings us to the end of the interview. Thank you again for taking the time to share your insights, it's been incredibly valuable for my research. As mentioned earlier, all responses will be anonymized and treated confidentially. If you would like to receive a summary of the findings or the final version of the framework, I'd be happy to share that with you once the thesis is complete. Before we finish, is there anything else you would like to add or clarify?