Semi-structured questions used in the first round interview with experts:

Cybersecurity risk management Experts

1. in your opinion, what are the key factors to consider when building a secure and functional HIoT BC-IdM system?
2. How do you manage security risks in applications based on evolving technology like Blockchain?
3. Blockchain is evolving, and systems based on it are distributed, therefore, when studying its security aspect, we need to study the whole ecosystem, do you agree?
4. In your opinion, how important is the evaluation phase in the decision-making process beside the security risk management? Especially when adopting Blockchain. What evaluation factors should include?
5. Do you think the provided framework aligns with security risk management frameworks such as ISO27005 and NIST800-39?
6. Do the proposed steps cover all the main elements of the cybersecurity risk management process? Do you suggest removing/adding phases/steps? Why?
7. Will the framework help to build a functional BC-IdM for HIoT and mitigate risks and support the decision-making process? Why?

BC technologies Experts

1. What BC infrastructure, other than Bitcoin/ Ethereum/ Hyperledger Fabric, do you consider has potential in BC-IdM systems? What are the comparison criteria?
2. What are the key factors when building a secure and functional BC-Identity management (IdM) system for applications like the Health Internet of Things (HIoT)?
3. What are the main evaluation factors for evaluating Blockchain-based applications, especially IdM systems?
4. What main entities are related to Blockchain-based applications (e.g., Blockchain infrastructure, developers, and users)? Especially in Blockchain -IdM systems?
5. What is your technical view on the proposed phases and steps in cybersecurity risk management? Any suggestions?
6. In your opinion, what other considerations need to be taken other than those mentioned in the framework concerning BC-IdM systems?
7. Will the framework help to build a secure and functional HIoT BC-IdM and mitigate risks and support the decision-making process? Why? Any suggestion for enhancement?

IdM systems Experts

1. What identity management (IdM) models are more applicable for HIoT, and which of these are the most secure in your opinion? What considerations need to be taken when selecting/applying them?
2. Are you familiar with decentralized IdM such as Blockchain-IdM applications? What is your technical perspective on that? What considerations need to be taken when considering Blockchain as a foundation for IdM systems, especially for the HIoT domain?
3. How do you think we can mitigate security and privacy risks in IdM systems? How about in HIoT BC-IdM?
4. What are the main functional, privacy, and security requirements of IdM systems? Are they covered in BC-IdM? How about for HIoT?
5. How BC-IdM systems can preserve users' security and privacy? How important of new BC-IdM systems being evaluated?
6. What are the evaluation factors and metrics to assess IdM systems/Blockchain-based IdM systems?
7. What is your technical view on the proposed phases and steps in cybersecurity risk management? Any suggestions?

Health IoT security Experts

1. What are HIoT IdM issues related to identification, authentication, and authorization?
2. What are the current HIoT IdM systems' pros, cons, and other considerations? Any thoughts about BC-based IdM systems and how they can be evaluated?
3. Are the current standards (international, national, technical) related to HIoT functionality and cybersecurity risks, enough? Do they consider emerging technologies like Blockchain?
4. How do you think we can mitigate security risks in HIoT BC-IdM systems?
5. What are HIoT applications' security, privacy, and functional requirements?
6. What are the impacted stakeholders when HIoT security and privacy are breached?
7. What is your technical view on the proposed phases and steps in the cybersecurity risk management framework? Are there important considerations missing?