**Response to Pok Chi Li:**

Hi Pok, thanks for your perspective on Industry 4.0, and for opening a discussion on the challenges organisations face in digital transformation. Your analysis of IoT and cloud computing provides valuable insights into two key technologies, though examining their interdependence would deepen our understanding of the broader technical ecosystem. For instance, how might IoT security vulnerabilities compound cloud computing risks, or how could integrated IoT-cloud solutions create new organisational challenges?

Your use of Shitta-Bey and Adewole's (2023) research effectively frames the technical risks in cloud computing. While you highlight crucial security concerns like API vulnerabilities that affect all industries, the impact and mitigation strategies can vary significantly across sectors. Healthcare organisations, for instance, might prioritise patient data protection, requiring particularly robust encryption and access controls, while manufacturers might focus on operational continuity and real-time threat detection to prevent production disruptions. This sectoral lens reveals why organisations need layered security approaches tailored to their specific context. Exploring these sector-specific challenges would strengthen your analysis – how might different industries prioritise and implement security measures? What unique risks emerge in sectors like finance, where real-time data accuracy is crucial, versus retail, where customer data protection is paramount?

Your examination of competence risks through Kovaitė and Stankevičienė (2019) raises crucial points about workforce readiness in digital transformation. While you effectively identify the challenge of staff lacking "comprehensive understanding," this could be explored more deeply – what specific competencies are most critical? How do these vary across different organisational levels? Your connection to Malewska et al.'s (2024) research on training and education offers a partial solution, but the relationship between training initiatives and risk mitigation could be more explicitly developed. For instance, how might targeted training programmes address specific competence gaps, and what metrics could organisations use to measure their effectiveness?

What makes your analysis particularly valuable is the potential connection between technical and human factors, though this could be developed further. Consider how improved digital literacy might lead to better security practices – for example, how staff trained in cybersecurity best practices could reduce API vulnerability risks. Similarly, examining how technical expertise shapes risk management strategies could provide valuable insights for organisations planning digital transformation initiatives.

**References:**

Kovaitė, K. and Stankevičienė, J. (2019) Risks of digitalisation of business models. *Proceedings of 6th International Scientific Conference Contemporary Issues in Business, Management and Economics Engineering '2019*.

Malewska, K. et al. (2024) *The missing link between digital transformation and business model innovation in energy SMEs: The role of digital organisational culture*. Available from: <https://www.sciencedirect.com/science/article/pii/S030142152400274X> [Accessed 30 Oct 2024]

Shitta-Bey, A. M., & Adewole, M. (2023). *Security concerns of cloud migration and its implications on cloud-enabled business transformation* (Doctoral dissertation, Università della Svizzera Italiana).