UNIT 1-2: COLLABORATIVE DISCUSSION 1

1. Industry 4.0 as defined by the authors

Kovaitė and Stankevičienė (2019) define Industry 4.0 as the integration of advanced digital technologies—such as the Internet of Things (IoT), big data analytics, cloud computing, and artificial intelligence— into interconnected systems that enable real-time communication and decentralised decision-making. Two practical examples include:

- Predictive maintenance in manufacturing using IoT sensors to monitor machinery health in real-time, reducing downtime.
- The application of big data in supply chains to optimise inventory and logistics decisions dynamically.

2. Risks associated with Industry 4.0

According to the authors (2019), Industry 4.0 present six distinct categories of risk that need to be addressed: technical, competence, acceptance by staff, acceptance by customers and partners, data privacy and security and financial risks. Two real-world examples mapped to the highest-impact risk areas identified by Kovaitė & Stankevičienė (2019) are:

- **Revenue streams – Financial and data security risk**
  Equifax's 2017 data breach compromised sensitive financial records, resulting in reputational damage and over $1.4 billion in settlement and security costs, directly impacting revenue streams (Federal Trade Commission, 2019).
- **Customer segmentation – Customer acceptance and data privacy risk**
  The Facebook–Cambridge Analytica scandal in 2018 raised public awareness of how personal data could be harvested and used without sufficient transparency, prompting debates on consumer trust, ethical data use, and regulatory oversight (Financial Times, 2018)

3. Supporting literature

Kovaitė and Stankevičienė (2019) make several key points:

- Industry 4.0-driven digitalisation introduces new and amplified categories of risk.

- These risks span multiple domains, including technological, human, organisational, and financial.
- The impact of risks is uneven, with certain business areas more exposed than others.
- Risks in Industry 4.0 are systemic and interconnected, allowing disruptions in one area to cascade to others.
- Understanding these impacts is essential for effective strategic planning.

Li (2024) supports the core concepts of Kovaitė and Stankevičienė (2019), particularly in recognising the multidimensional and interconnected nature of Industry 4.0 risks. Like Kovaitė and Stankevičienė, Li identifies distinct risk categories — technological, organisational, environmental, and regulatory — and acknowledges that the impact of these risks is not uniform across the organisation. Li specifically highlights that certain business areas, such as supply chains and customer-facing services, are more exposed to digitalisation risks. Additionally, Li underscores the interconnectedness of these risks, demonstrating how a technical failure can escalate into operational disruptions and reputational damage.

However, the studies differ in their strategic focus. While Kovaitė and Stankevičienė map risks to business model components for strategic adaptation, Li prioritises risks to enhance innovation success and organisational resilience. Li uses a fuzzy multi-criteria decision-making (MCDM) approach to rank risks based on their influence, contrasting with K&S's use of the FARE method to categorise and map risks.

In conclusion, Li (2024) strongly supports the core points made by Kovaitė and Stankevičienė (2019), validating their findings while offering a complementary approach that focuses on risk prioritisation for strategic innovation and resilience.

Reference list

Federal Trade Commission (2019) *Equifax to pay $575 million as part of settlement with FTC, CFPB, and states related to 2017 data breach*. Available at: https://www.ftc.gov/news-events/news/press-releases/2019/07/equifax-pay-575-million-part-settlement-ftc-cfpb-states-related-2017-data-breach (Accessed: 30 July 2025).

Financial Times (2018) *What impact will Facebook scandal have? Full transcript of FT City Network debate*. Available at: https://www.ft.com/content/666d50ae-47dd-11e8-8ae9-4b5ddcca99b3 (Accessed: 30 July 2025).

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*. Available at: https://doi.org/10.3846/cibmee.2019.039 (Accessed: 30 July 2025).

Li, X. (2024) 'Navigating digital transformation: a risk-based approach for Industry 4.0 innovation', *Journal of Enterprise Information Management*, 37(5), pp. 1271–1293. Available at: https://doi.org/10.1108/JEIM-07-2023-0325 (Accessed: 30 July 2025).

Peer 1 reaction

Dear [redacted],

Your comprehensive analysis effectively captures the multidimensional nature of Industry 4.0 risks as conceptualized by Kovaitė and Stankevičienė (2019). Your definition appropriately emphasizes the interconnected systems and real-time decision-making capabilities that distinguish Industry 4.0 from previous industrial paradigms. The predictive maintenance and supply chain optimization examples you provided clearly demonstrate the practical applications of these integrated digital technologies.

Your risk categorization and real-world examples are particularly insightful. The Equifax breach exemplifies how data security vulnerabilities can cascade into significant financial implications, whilst the Facebook-Cambridge Analytica scandal aptly illustrates the intersection of customer acceptance and data privacy risks. These examples effectively demonstrate the interconnected nature of Industry 4.0 risks that Kovaitė and Stankevičienė emphasize.

The incorporation of Li's (2024) comparative analysis strengthens your argument considerably. However, your discussion could benefit from exploring additional dimensions of risk interconnectedness. Ghobakhloo (2020) argues that Industry 4.0 implementation creates "risk amplification effects" where traditional operational risks become more severe due to increased system dependencies. This perspective suggests that beyond the six categories identified by Kovaitė and Stankevičienė, organizations must also consider how digitalization fundamentally alters the risk landscape rather than merely introducing new risk types.

Furthermore, whilst Li's fuzzy MCDM approach offers valuable risk prioritization insights, Raj et al. (2020) contend that dynamic risk assessment frameworks are essential given the rapid evolution of Industry 4.0 technologies. This temporal dimension of risk management warrants consideration alongside the spatial mapping approach you've outlined.

Your analysis effectively demonstrates the scholarly consensus regarding Industry 4.0's complex risk profile whilst highlighting methodological variations in risk assessment approaches.

Lis of References:

Ghobakhloo, M. (2020) 'Industry 4.0, digitization, and opportunities for sustainability', *Journal of Cleaner Production*, 252, 119869.

Raj, A., Dwivedi, G., Sharma, A., de Sousa Jabbour, A.B.L. and Rajak, S. (2020) 'Barriers to the adoption of industry 4.0 technologies in the manufacturing sector', *Computers & Industrial Engineering*, 148, 106706.

Peer 2 reaction

Hi [redacted],

Your post gave a clear breakdown of how Kovaitė and Stankevičienė (2019) define Industry 4.0 and its associated risks. I agree with your interpretation that the integration of IoT, big data, and AI is central to creating interconnected systems capable of decentralised decision-making. The examples you provided, such as predictive maintenance and dynamic supply chain optimisation, illustrate how these technologies can directly improve operational efficiency and reduce costs when implemented effectively.

The real-world cases you mentioned, particularly the Equifax breach and the Facebook–Cambridge Analytica incident, are strong illustrations of how data security and privacy risks can quickly escalate into significant financial and reputational damage. I think these examples also highlight that technical measures alone are insufficient. Organisational culture, transparent communication, and ongoing staff training play a key role in mitigating such incidents.

I also found your comparison between Kovaitė and Stankevičienė's use of the FARE method and Li's (2024) fuzzy MCDM approach interesting. It shows how different methodologies can lead to complementary insights. In my view, combining elements of both could provide a more robust risk assessment framework by allowing for both risk categorisation and prioritisation.

It might also be useful to consider emerging regulatory frameworks, such as the EU's AI Act, which could influence how organisations address Industry 4.0 risks going forward. These evolving regulations could significantly affect both customer acceptance and operational processes.

Overall, your analysis was well-structured and provided a balanced view of both opportunities and risks.

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*. Available at: https://doi.org/10.3846/cibmee.2019.039 (Accessed: 30 July 2025).

Li, X. (2024) ‘Navigating digital transformation: a risk-based approach for Industry 4.0 innovation’, *Journal of Enterprise Information Management*, 37(5), pp. 1271–1293. Available at: https://doi.org/10.1108/JEIM-07-2023-0325 (Accessed: 30 July 2025).

Tutor response

Wonderful initial post!