**Summary Post – Risk Assessment in Industry 4.0 System**

The fourth industrial revolution also known as Industry 4.0 involves a fusion of technologies that are blurring the lines between the physical, digital, and biological spheres (Schwab, 2016). Kovaitė and Stankevičienė (2019) opined that the industry 4.0 encompasses a range of technological drivers as the Internet of things (IoT), big data, cloud computing, robotics, artificial intelligence and explores the decentralisation of communication between people and machines. These Industry 4.0 technologies can be applied in supply chain management and predictive maintenance among other applications. Embracing Industry 4.0 opens a myriad of benefits and risks for businesses. These risks can be classified into technical, competence, behavioural, data security and financial risks (Kovaitė & Stankevičienė, 2019). Behavioural risks can be further classified into 2, namely, risks related to staff competence (internal) and risks related to customers' and partners' attitude.

An insufficiently trained staff can be a source of risk (behavioural) to the business. Likewise rapid technological changes and inadequate knowledge could result in significant risks (competence risks) not being identified and subsequently mitigated. Furthermore, with increasing complexity and automation, existing standards and methodologies may be inadequate for risk management. It was on this basis that Kovaitė and Stankevičienė (2019) developed the Risk Assessment of Digitalisation of Business (RADi) model for identification of areas of highest risks in business models driven by Industry 4.0. Similarly, Nurse, Creese & Roure (2017) opined that simply extending existing methodologies to Industry 4.0 systems could result in blindness to new risks arising in such ecosystems. For

example, the General Data Protection Regulation (GDPR) could be limited in managing risks in blockchain technology. This is because of the immutable nature of the blockchain (Ombir, 2022). Any modification to one block could potentially render all successive blocks invalid. This violates users' rights under the GDPR to erase, review, and transfer their personal data. Overall, Industry 4.0 significantly affects how risk assessment is carried out.

## References


Kovaitė , K., & Stankevičienė, J. (2019). Risks of digitalisation of business models. Available from https://www.researchgate.net/publication/333063956_Risks_of_digitalisation_of_business_models [Assessed 12 August 2022].

Lucian, A., John, K., & Onesmo, S. (2020). Benefits of Industrialization. Available from https://www.efdinitiative.org/publications/benefits-industrialization [Assessed 12 August 2022].

Nurse, J., Creese, S., & Roure, D. (2017). Security risk assessment in Internet of Things systems. Available from https://kar.kent.ac.uk/67476/ [Assessed 12 August 2022].

Ombir, S. (2022). How Does GDPR Impact Emerging Technologies? Available from https://datafloq.com/read/how-does-gdpr-impact-emerging-technologies-2/ [Assessed 27 August 2022].

Schwab, K. (2016). The Fourth Industrial Revolution: what it means, how to respond. Available from https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/ [Assessed 12 August 2022].