Unit 5 – Collaborative Wiki Development: The Future of ISM

Title: Which factor will most affect the future direction of Security and Risk Management?

1. **How can we describe and represent the results of risk assessments in a way that is useful to decision-makers, which clearly presents the assumptions made and their justification with respect to the knowledge upon which the assessment is based?**

Nowadays, most social sectors use techniques and methodologies to assess and manage risks. Risk management has two primary responsibilities - reviewing and operating the risks associated with specific activities and conducting general research and development to understand, evaluate, manage, and control risk (Aven, 2016).

Aven (2016) highlights that risk assessment and management face significant uncertainties, including emerging risks related to black swan-type events. Therefore, it is crucial to accurately represent risk information, account for uncertainties, and develop modelling methods to handle complex systems.

Hu et al. (2021) emphasise that establishing a common understanding of risk among stakeholders is crucial. This enables consistent decision-making in specific circumstances and gives stakeholders and the public access to actionable, transparent risk indicators and critical goals of effective risk communication. It is vital to ensure stakeholders know the importance of risk assessment, its purpose, and how to use it to guide choices. Predictions of actuarial risk can enhance data-driven decision-making and yield better results.

According to Bier (2001), decision-makers must receive thorough, reliable, and intelligible risk assessment data relevant to particular risk management policy frameworks for risk communication to be effective. When making decisions related to

risk, decision-makers should consider legal requirements, possible negative impacts, strategies for reducing risk, the degree of concern, and the accuracy of information. Effective risk communication can assist decision-makers in determining the public's most likely reactions to different possibilities for decision-making.

This process includes identifying the risk, assessing its likelihood and impact, communicating the risk transparently and truthfully, managing the risk effectively, and monitoring the results of the risk communication strategy over time (SafetyCulture, 2022).

ZebraBI (2023) claims that well-planned presentations can effectively warn audiences of potential risks. Include charts, graphs, and other visual aids to make the content easier to understand. It's essential to avoid technical jargon that might confuse the audience. Thus, narrative descriptions provide a detailed analysis of each risk while accounting for its likelihood, affected areas, and potential consequences. Also, any presumptions formed throughout the assessment should be made clear.

Effective communication and visualisation are necessary for project risk management to ensure decision-makers understand the risks. The use of graphics and visual aids is crucial in presenting complex information to support the decision-making process. However, traditional risk assessment matrices have limitations, including the lack of interdependency between risks and the failure to consider the aggregated impact of risks on multiple project objectives (Atasoy et al., 2022). In addition, risk management professionals use a risk register to track organisational risks. They often use a risk matrix or heat map to communicate risk concepts to senior leaders (College Sidekick, 2024).

Properly informing decision-makers of the risk assessment findings is crucial to ensure informed decision-making. Depending on the target audience, Fraser & Simkins (2016) have highlighted the following techniques to do this:

- Organisations use enterprise risk management (ERM) when reporting to leadership to ensure the teams in charge of the firm are aware of the risks that might compromise its goals. Creating an initial risk profile is one of the most essential parts of writing to leadership. In smaller businesses, risk workshops might be used to introduce ERM. Executive team members would discuss potential risks and rank them according to the need for further action.

- A committee that the board assigns responsibility for risk supervision should regularly ask management for risk profiles. These profiles often include risk maps, lists of the top 10 risks, and heat maps, all enhanced by narratives that explain the origins of the risks, the objectives they affect, and the measures that have been taken or are being considered.

- The board should examine if any board committee is doing more thorough supervision, as there is disagreement over the amount of information and time the board should devote to risk management.

Lyon & Popov (2017) state that maintaining effective communication is crucial when managing operational risk. According to ANSI/ASSE 2, continuous and iterative processes must be implemented to provide, share, or obtain information with stakeholders regarding risk management. The consequences of inadequate communication can be severe, as demonstrated in events like the Toyota Worldwide vehicle recall and the Deepwater Horizon oil spill.

Risk-Based Decision Making (RBDM) is a structured process that enables decision-makers to make informed choices. This process considers the possibility of undesired outcomes, the probability and severity of potential outcomes, and whether risk reduction is necessary. The five steps of RBDM include identifying decision parameters, evaluating risk, making an informed decision, monitoring effectiveness, and facilitating communication. OSH professionals can effectively communicate risk

using various risk assessment methods, such as HAZID, RISKID, RAM, heat map, PHA, LOPA, striped bow tie risk assessments, and cascading bow-tie diagrams (Lyon & Popov, 2017).

2. What trend will significantly influence the most in the next five years?

Edge computing is a technology that is predicted to have a significant impact on the technology industry within the next five years, as per Pratt's (2024) statement. The Industry Outlook Report (2024) further states that the Edge Computing market is expected to grow exponentially due to the increasing demand for sustainable products and the widespread adoption of cutting-edge technologies like artificial intelligence, machine learning, and blockchain. The market offers various products and services, mainly hardware and software, and is growing due to multiple factors such as transportation, logistics, manufacturing, healthcare, IT, and telecom. The report provides valuable information on market segmentation, growth opportunities, and major players. The market is expected to reach multimillion figures by 2030, showing an unexpected compound annual growth rate. The leading regions in this market are North America, Europe, Asia-Pacific, Latin America, and the Middle East & Africa.

Edge computing processes client data at the network's edge, meaning storage and compute resources are moved closer to the data source. This allows for real-time processing and reduces latency and bandwidth limitations. Edge computing is transforming how businesses approach computing and reshaping IT and business computing (Bigelow, 2021).

Ashtari (2022) highlights that edge computing brings computer processes and data storage closer to organisations, reducing response times and bandwidth usage. It also improves cybersecurity, increases computer speed, and lowers the cost of data

storage. Adopting edge computing can lead to global strategic innovations and growth in industry data analytics.

Edge computing captures and processes data close to its source to minimise latency and data transit costs, allowing real-time feedback and decision-making. This is especially important for applications where human safety is a factor, such as self-driving cars and hospitals. While edge computing is essential for modern AI applications, it is not a new concept (Yeung, 2019).

Frank L. (2023) notes that edge computing requires a distributed system with a large attack surface that is particularly susceptible to attacks. Due to a single IoT device, the network as a whole may be vulnerable to attacks and security lapses. Furthermore, edge computing risks the entire system by making verifying data and managing user devices challenging. Moreover, edge computing is often employed in high-risk, life-threatening applications, including autonomous vehicles, goods warehouses, and healthcare systems that require sophisticated processing.

Nolle (2021) offers six fundamental guidelines to guarantee the security of edge computing operations. These include increasing perimeter physical security, moving operation control and edge configuration centrally from IT operations, implementing stringent auditing protocols, employing robust network security, securing the edge using its tools and procedures, and keeping an eye on and documenting all edge activity, particularly operations and configuration. Additionally, organisations should supervise all edge setup and operations rather than local staff, and access to edge facilities must be restricted. Every edge application and data hosting should adhere to auditing regulations and be under central management.

Lastly, confirming that the network connection is entirely secure using multifactor authentication, high-grade encryption, or a physical security dongle for all network, application, and operation access is crucial. Wi-Fi resources must be located on a different network, and any edge computing activity must be tracked, recorded, and examined (Nolle, 2021).

References:

- Aven, T. (2016). Risk Assessment and Risk management: Review of Recent Advances on Their Foundation. *European Journal of Operational Research*, [online] 253(1), pp.1–13. Available at: https://doi.org/10.1016/j.ejor.2015.12.023.
- Hu, C., Roberts, K., Jannetta, J. & Kim, K. (2021). *Communicating Risk Information for Effective Decisionmaking*. [online] Available at: https://www.urban.org/sites/default/files/publication/103865/communicating-risk-information-for-effective-decisionmaking.pdf.

- Bier, V.M. (2001). On the state of the art: risk communication to decision-makers. *Reliability Engineering & System Safety*, 71(2), pp.151–157. doi:https://doi.org/10.1016/s0951-8320(00)00091-0.
- SafetyCulture (2022). *Risk Communication: Why Is It Essential?* [online] SafetyCulture. Available at: https://safetyculture.com/topics/risk-communication/.
- ZebraBI (2023). *How to Perform Risk Assessment in PowerPoint - Zebra BI*. [online] Available at: https://zebrabi.com/guide/how-to-perform-risk-assessment-in-powerpoint/ [Accessed 28 Feb. 2024].
- Atasoy, G., Ertaymaz, U., Dikmen, I. & Talat Birgonul, M. (2022). Empowering Risk Communication: Use of Visualizations to Describe Project Risks. *Journal of Construction Engineering and Management*, 148(5). doi:https://doi.org/10.1061/(asce)co.1943-7862.0002265.
- College Sidekick (2024). *Chapter 3 Information Risk Management*. Available at: https://www.collegesidekick.com/study-docs/1709184. [Accessed 28 Feb. 2024].
- Fraser, J.R.S. & Simkins, B.J. (2016). The challenges of and solutions for implementing enterprise risk management. *Business Horizons*, [online] 59(6), pp.689–698. Available at: https://ideas.repec.org/a/eee/bushor/v59y2016i6p689-698.html.
- Lyon, B. K. & Popov, G. (2017). Communicating & Managing Risk The Key Result of Risk Assessment. Available at: https://www.assp.org/docs/default-source/psj-articles/f2_1117.pdf?sfvrsn=3b44fd47_2. [Accessed 01 Mar. 2024].
- Pratt, M. K. (2024). *5 edge computing trends to watch in 2022 and the future*. [online] Available at: https://www.techtarget.com/searchcio/tip/Top-edge-computing-trends-to-watch-in-2020.
- Industry Outlook Report (2024). *Edge Computing Market Challenges (2023-2030)*. [online] Available at: https://www.linkedin.com/pulse/edge-computing-market-challenges-2023-2030/ [Accessed 4 Mar. 2024].
- Bigelow, S.J. (2021). *What Is Edge Computing? Everything You Need to Know*. [online] Techtarget. Available at: https://www.techtarget.com/searchdatacenter/definition/edge-computing.
- Ashtari, H. (2022). *Edge Computing vs. Cloud Computing: 10 Key Comparisons*. [online] Available at: https://www.spiceworks.com/tech/cloud/articles/edge-vs-cloud-computing/.
- Yeung, T. (2019). *What Is Edge Computing?* [online] NVIDIA Blog. Available at: https://blogs.nvidia.com/blog/what-is-edge-computing/ [Accessed 1 Mar. 2024].
- Frank L. (2023). *Edge Computing Security: Risks, Considerations, and Best Practices*. [online] Available at: https://getstream.io/blog/edge-computing-security/.
- Nolle, T. (2021). *Edge computing security risks and how to overcome them*. [online] IoT Agenda. Available at: https://www.techtarget.com/iotagenda/tip/Edge-computing-security-risks-and-how-to-overcome-them.