Unit 4 : Risks and risk mitigation

Formative Activity	Review the article by Anton & Nucu (2020) and consider risk models for the SDLC

Enterprise Risk Management (ERM) allows organisations to identify, evaluate and manage risk. According to Anton and Nucu, factors motivating firms to engage with risk management are:

- Financial distress
- Low earnings
- Barriers to growth
- Independence of the board

The article is primarily focused on the financial risks, which while critical to any business is represent an important, but narrow lens from which to view risk. Risk to business will be associated with the strategic goals of the organisation which may address corporate responsibility, or community cohesion. Not all business goals are financial and it may be that the some financial goals are secondary to the values of an organisation.

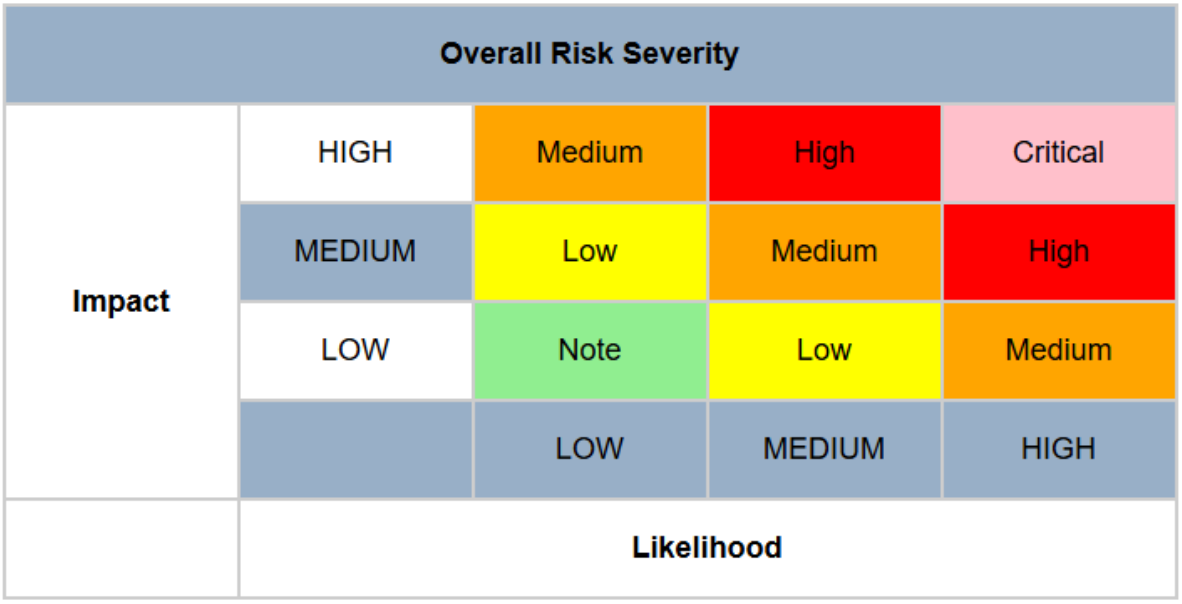
There may be more suitable risk frameworks associated with the Software Development Lifecycle such as the OWASP Risk Rating Methodology. This methodology adopts a standard definition that Risk = Likelihood * Impact. These measures need to be easily understood, so a simple scale from 0 to 9 is used for both likelihood and impact where:

- 0 to <3 :Low
- 3 to <6: Medium
- 6 to 9: High

OSWAP advise deafferenting between technical and business impact which is a more nuanced and appropriate response. Furthermore, the recommendation is that the business risk should supersede the technical risk when considering mitigation.

Finally, severity is defined using the matrix below:

Figure 1: Severity Matrix



The severity matrix neatly summarises the complexities of risk, allowing high-level communication to all stakeholders.

In summary, the OWASP Risk Assessment Methodology represents an ideal risk framework for the SDLC process as:

- Technical and Business risks are assessed
- Technical risks are places in the overarching context of the business
- Severity can be easily shared with all stakeholders.

References

Anton, S. G., & Nucu, A. E. A. (2020). Enterprise Risk Management: A Literature Review and Agenda for Future Research. *Journal of Risk and Financial Management*, *13*(11), 281. https://doi.org/10.3390/jrfm13110281

Williams, J. (no date) *OWASP Risk Rating Methodology*. OWASP Foundation. Available at: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology [Accessed 8 June 2025].