Wiki Entry: Risks and Risk Mitigation – Anton & Afloarei Nucu (2020)

1. Main risks identified in Anton & Afloarei Nucu (2020) and how they fit into the SDLC

Anton and Afloarei Nucu (2020) conduct a systematic literature review of Enterprise Risk Management (ERM) and therefore do not present their own taxonomy of risks. Instead, they synthesise findings from empirical studies that identify enterprise-level risk motivators for ERM adoption. A key referenced study, Khan et al. (2016, cited in Anton & Afloarei Nucu, 2020), identifies the following risk drivers:

- Probability of financial distress
- Low earnings performance
- Growth-opportunity vulnerabilities
- Lack of board independence / weak governance

These risk types can be mapped to the traditional Software Development Life Cycle (SDLC) as follows:

Planning & Analysis: Financial distress and weak governance can lead to unstable budgets, unrealistic scoping, and poor requirements decisions.

Design & Implementation: Growth-opportunity risks and weak board oversight reduce organisational responsiveness, limiting architectural quality and increasing the likelihood of technical debt.

Testing & Maintenance: Low earnings performance often correlates with underinvestment in long-term quality, scalability and maintenance, increasing operational and security risks after deployment.

2. Framework for capturing and categorising the risks

From the Unit 3 lecturecast, the Risk Management Process (RMP) framework encompasses four core phases: identification, analysis, evaluation and treatment. This framework is particularly suitable for capturing Anton & Nucu's identified enterprise risks because it:

- **Identification phase:** Systematically surfaces financial, governance and strategic growth risks across all organisational systems (strategy, structure, technology, intellectual resources)
- **Analysis phase:** Examines how each risk (e.g. weak board independence) propagates through SDLC phases and impacts budget stability, architectural decisions and long-term maintenance costs
- **Evaluation phase:** Prioritises risks by likelihood and impact, aligning with organisational risk appetite
- **Treatment phase:** Develops mitigation strategies tailored to each SDLC phase

This approach aligns with the Hoffmann et al. (2016) model discussed in the lecturecast, which treats the organisation as an integrated system of strategy, structure, technology, intellectual resources and management systems.

3. Risk + suggested mitigation (Wiki contribution)

Risk: Fragmented ERM governance resulting in unclear risk ownership across SDLC phases.

Mitigation: Establish formal risk ownership roles aligned to the SDLC phases (Planning Risk Owner, Development Risk Owner, Deployment Risk Owner). Integrate risk identification, analysis and evaluation checkpoints at each SDLC phase gate to prevent decision-making gaps and ensure continuity of enterprise-level oversight, following the RMP treatment and monitoring protocols.

References

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

Hoffmann, R., Kiedrowicz, M. and Stanik, J. (2016) 'Risk management system as the basic paradigm of the information security management system in an organization'. Available at: https://doi.org/10.1051/MATECCONF/20167604010