Risk Analysis

There are two components to risk management, being assessment/analysis and mitigation of risk. Risk analysis identifies, quantifies or qualitatively define risks, and through established evaluation criteria, risks are prioritised (Nieles et al., 2017).

Quantitative Risk Analysis

The quantitative risk analysis method estimates the value of the assets using numerical calculation related to each component resulting from the risk assessment (Ramona, 2011).

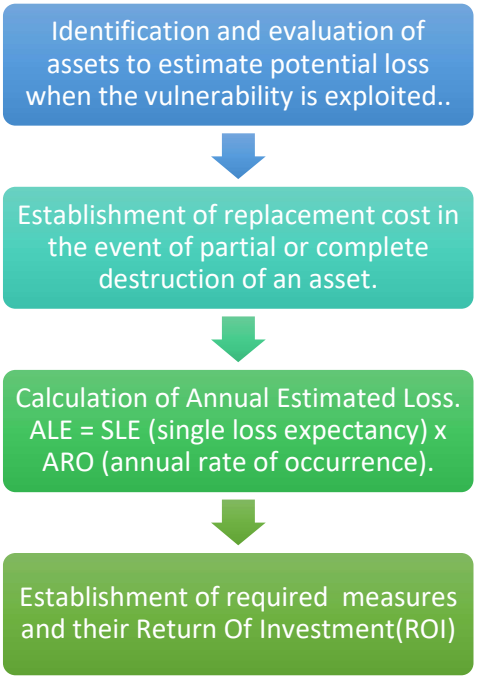

Figure 1: Quantitative Risk Analysis Approach steps.

Qualitative Risk Analysis

In qualitative risk analysis, relative values are used as inputs to estimate the impact or the value of the potential loss instead of statistical values. High/often, significant, and low/rare refer to the risk occurrence probability and impact. For classification of the information, words such as general, crucial, critical are used (Sung, 2015).

Figure 2: Qualitative Risk Assessment Method Steps.

We chose the qualitative assessment method for the assessment. Our choice of qualitative methodology is because the approach simplifies understanding and observation of the level of risk, understanding and implementation of calculation methods are simple. The approach also allows for the determination of areas of greater risk in a short time and without a more significant expenditure, and analysis is relatively inexpensive and straightforward (Simmons et al., 2017). Without a comprehensive knowledge of the complete list of assets and the absolute value of the business, it won't be easy to use the quantitative approach since its input are majority numerical.

Risk Identification

Probability and Impact Scales.

Table 1: Probability Scale.

Probability of Risk Occurrence	Occurrence Criteria(Classification, Probability of Risk Event)
None (0)	Not Applicable.
Rare(1)	=< 20%
Unlikely(2)	>20% - =<40%
Possible(3)	>40% - =<60%
Likely(4)	>60% - =<80%
Frequent(5)	>80%

Table 2: Impact Scale.

Financial and Reputational Impact	Budgetary and Reputational Implications (Finacial Impact; Reputational Impact)
None	Not Applicable.
Low	(<$10,000/ Internal IT stakeholders aware of risk event occurrence)
Moderate	($10,001 - $25,000/ Business Customers are aware of risk event occurrence)
High	($25,000 - $50,000/ Board of directors are aware of risk event occurrence)
Very High	($50,000 - $100,000/External customers are aware of the risk event occurrence)
Extreme	(>$100,000/Media coverage or regulatory body are aware of risk event occurrence)

Risk Severity Scale.

According to the NIST SP 800-30 methodology, the process of risk assessment consists of nine(9) primary phases (Joint Task Force, 2018) :

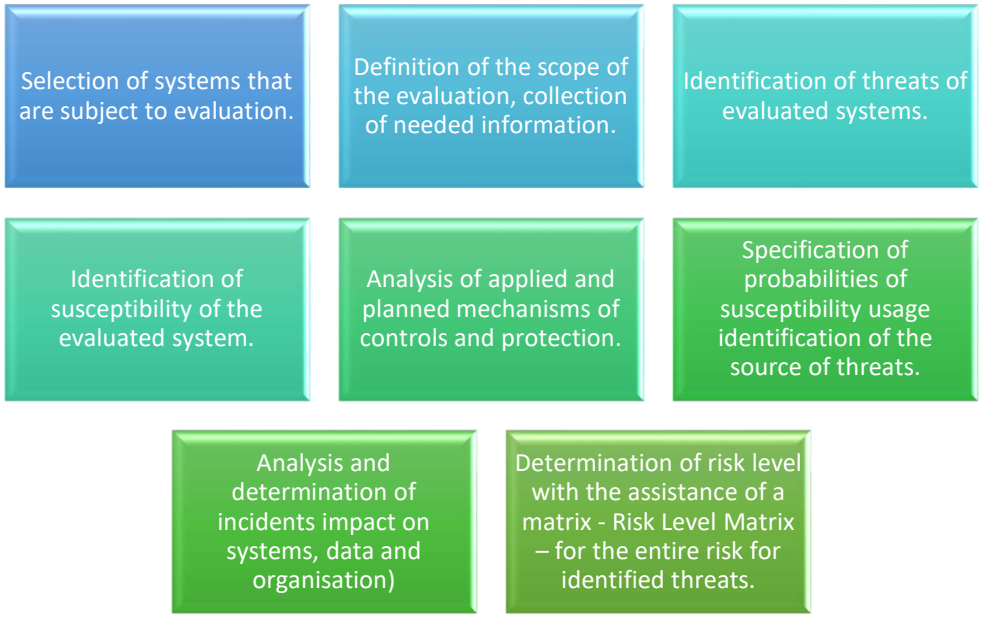

Figure 3: NIST SP 800-30 Methodology.

The following Risk Matrix was derived from multiplying the probabilities (in Table 1: Probabilities Scale.) with the impact(in Table 2: Impact Scale)

Table 3: Risk Level Matrix

	Financial Risk Severity Matrix					
		Low	Moderate	High	Very High	Extreme
Probability.	Rare	Low	Low	Low	Moderately Low	Moderate
	Unlikely	Low	Moderate	Moderately High	Moderately High	High
	Possible	Moderate	Moderately High	High	Very High	Very High
	Likely	Moderate	Moderately High	High	Very High	Extreme
	Extreme	Moderate	High	Very High	Extreme	Extreme

Risk Register.

The risk register below was derived from identifying risk factors/categories and the level of risk that initiating events or actions carry.

Table 4: Risk Register with Risk Levels.

Risk Category	Risk Factor	Risk Level
Strategic	Misalignment with overall Information Technology Architecture.	High
Technical	Not meeting system's IT(software, hardware, network, and security) requirements/specifications.	Low
Operational	Business case' outlined benefits not met.	Moderate
Project Management	Necessary project resources have not been available.	Moderately High
Organisational Fit	Failure to reengineer business processes.	Moderate
Management	Inadequate communication system.	Moderate
Operational	Lack or no disaster recovery plan.	High
Management	No Risk management process.	High
Strategic	Unclear objectives /Inadequate ERP implementation strategy.	High
Strategic	Inadequate measure to align with Sarbanes-Oxley Act(SOX)	Low
User involvement and training.	Insufficient end-user training.	Moderate
User involvement and training.	Insufficient sensitivity to user resistance.	Moderate
Technical	Incorrect ERP package selection.	High
Project Management	Quality deficiency as a result of time/cost drivers.	Moderately High
Strategic	The system produced data fails to comply with Data Protection Regulations.	Low

Risk Management Strategies Mapping with SDLC(Systems/Software Development Life Cycle)

Table 5: Risk Management mapping with SDLC.

SDLC Phase	Risk
Planning(identification, classification and prioritisation of the problem)	• Poor and conflicting ERP system requests. • Poor planning. • Consistent changes in requirements. • Lack of clarity of objectives and goals.
Analysis	• Misalignment with overall Information Technology Architecture. • Definition and evaluation of performance requirements
Design	• Poor communication. Lack of understanding of the requirements. • Insufficient internal expertise in ERP systems development. • Inadequate documentation. • Insufficient competence of ERP consultants. •
Implementation	• Poor alignment with standard process/methodology/procedures. • Poor organisational maturity level. • Poor technical infrastructure. • Complex and challenging procedures.
System Testing	• Business case' outlined benefits not met. • The system produced data fails to comply with Data Protection Regulations. • Inappropriate System Testing. • Inadequate tools and technology for testing. • Alignment and adherence failure to standardised specifications which the software supports. • Integration failure.
Acceptance Testing	• Lack of permanent commitment of users to project management and project activities. • Poor quality standard measurements. • Lack of management support.
Delivery	• Insufficient training of ERP end-users. • Lack of supporting documentation for ERP end-users.

References :

Aloini, D., Dulmin, R., & Mininno, V. (2007). Risk management in ERP project introduction: Review of the literature. *Information and Management*, *44*(6), 547–567. https://doi.org/10.1016/j.im.2007.05.004

Dey, P. K., Clegg, B., & Cheffi, W. (2013). Risk management in enterprise resource planning implementation: A new risk assessment framework. *Production Planning and Control*, *24*(1), 1–14. https://doi.org/10.1080/09537287.2011.597038

Joint Task Force. (2018). SP 800-037, Rev.2, Risk Management Framework (RMF) for Information Systems and Organisations. *NIST Special Publication - 800 Series*, 183. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final%0Ahttps://doi.org/10.6028/NIST.SP.800-37r2

Lopez, C., & Salmeron, J. L. (2011). A framework for classifying risks in ERP maintenance projects. *ICE-B 2011 - Proceedings of the International Conference on e-Business*, 201–204. https://doi.org/10.5220/0003407802010204

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST Special Publication 800-12 Revision 1 - An introduction to information security. *NIST Special Publication*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Ojala, M., Vilpola, I., & Kouri, I. (2006). Risks in ERP project - Case study of IS/ICT management capability maturity level and risk assessment. *Proceedings of the International Conference on Electronic Business (ICEB)*.

Ramona, S. E. (2011). Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches. *Chinese Business Review*, *10*(12), 1106–1110. https://doi.org/10.17265/1537-1506/2011.12.002

Simmons, D. C., Dauwe, R., Gowland, R., Gyenes, Z., King, A. G., Riedstra, D., & Schneiderbauer, S. (2017). Qualitative and quantitative approaches to risk assessment. *Understanding Disaster Risk: Risk Assessment Methodologies and Examples*, 44–130.

Sung, S. H. (2015). Quantitative and Qualitative Approach for IT Risk Assessment. *Asia-Pacific Journal of Convergent Research Interchange*, *1*(1), 29–35. https://doi.org/10.21742/apjcri.2015.03.04

Thangamani, G. (2018). Practical Risk Assessment Methodology for ERP Project Implementation. *Journal of Economics, Business and Management*, *6*(3), 84–90. https://doi.org/10.18178/joebm.2018.6.3.555