

Business scenario overview

Acme currently has an existing model of spreadsheets. However, due to the increased demand, these have become unmanageable because they are time-consuming and vulnerable to human errors. Purchasing an ERP is ideal as it will facilitate effective resource planning and scheduling. Hence we recommend COTS.

Justification

-Developed by the primary manufacturer with the assumption that the manufacture has all expertise and skills and that the system is flawless.

-Open-source solution relies on the community for escalation, and that might mean you will only get support later when someone in the community responds

A student's in-house created solutions might have many flaws, resulting in loss of clients, reputation, and personal data.

Cost-benefit analysis

Although COTS is expensive, its benefits far outweigh those of the other two systems. Post-implementation costs of open source and in-house solutions may amount to more than \$100k per annum. Since these systems do not have manufacturer support for instances where the system is faulty, there is no guarantee of money back. Systems made from amateurs may also result in loss of sales leading to loss of revenue if they are not properly designed, tested and secured. Due to this, millions may be lost online from cyber-crimes.

The information provided in Acme Manufacturing's supply chain needs to be analysed regarding developments for various sectors. It is essential to evaluate the knowledge base on risks and uncertain product and supply chain functions. It is necessary to go further than just risk assessment and combine the risk information received from the company with data from other sources involving other targets. Political issues can also be analysed on risks and safety that are not necessarily addressed by the project review (Aven, 2016).

Business challenges and rationale

Risk management has a significant challenge between the fast growth of technologies and the complexity of the risk management requirements. The business should create standardisation documents for all new system deployments to cover all risk management expectation issues and minimise any lack of communication between the business departments. Business challenges would be:

- Understanding the critical risk of terms.
- Understanding the risk assessment rules.
- Get the proper support from high-level management to determine risk strategy and make correct decisions.
- Understanding the technical architect for the whole organisation.
- Follow the correct risk measurement and force all departments to follow the correct process of risk treatment.
- Untrained personnel for the system
- Staff who resist change

Managing and monitoring all the risks using convenient tools can alert the risk managers for any issues.

The considerable important work in risk management is creating the business's disaster recovery and ensuring the organisation can get back into work immediately and has the plan to store and recover all records. All disaster recovery planning should contain a recovery point objective(RPO) and recovery time objective(RTO) to help minimise the downtime the business can handle.

Discussion and selection of tools

We have opted for a high-level three-phase approach for the ERP implementation risk management – (1) planning,(2) implementation and (3) post-implementation. The stages for accomplishing this process derived from the Open Process Framework are: identifying and classifying risk, analysing risk, developing an approach to identified risk, tracking risk, and treating risk. We categorised risks' main areas as technical, operational, management, strategy, and schedule.

TOOLS AND PRACTICES.

- Risk Breakdown Structure (RBS), a tool for risk identification, will be used to identify risks.
- PEST, CRAMM and OCTAVE frameworks are risk tools that we intend to use.
- The risk manager will maintain a risk register combined with a risk log and be subjected to review as an agenda item for risk management meetings.
- We will use a risk management manual to establish a nominal group technique and a risk matrix

-We also intend to use risk theories of continuous risk monitoring and specific risk management policies.

TIMELINE

Risk Assessment Timeline		Month						
		Day	1-2	3-4	5	6	7-9	9-11
		Week	1			2		
KEY								
PLANNED VS ACHIEVEMENT		PLANNED TIMELINE CODE						
		COMPLETED ON SCHEDULE						
		COMPLETED OUTSIDE SCHEDULE						
		ONGOING						
		BEHIND SCHEDULE						
ACTIVITY								
1	Identification of Risks							
2	Analysis of risk and challenges							
3	Prioritisation of risks							
4	Recommendation of system							
5	Creation of disaster recovery solution							
6	Submission of report							

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>

Aven, T. (2016) Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1-13. Available from: <https://doi.org/10.1016/j.ejor.2015.12.023> [Accessed 25 August 2021].

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>

Leopoulos, V., Kirytopoulos, K., & Voulgaridou, D. (2006). A model for risk identification in ERP system processes. *WIT Transactions on Ecology and the Environment*, 91, 143–152. <https://doi.org/10.2495/RISK060141>

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>