Status Report Document for IRM of Acme Manufacturing

Challenges as a niche company and role of an integrated ERP system

Acme manufacturing as an SME (Small/Medium Enterprise) producing sporks to a niche market, has its own challenges and opportunities to be successful as a sustainable business model.

According to its market definition being idiosyncratic, leading a small team of 150 members, while serving customer needs, often demands a flexible organisation setup with an ability to customise products.

The current practice of having a spreadsheet as a solution for all resource planning and scheduling is becoming cumbersome due to evolving market dynamics and demands.

Acme has decided to pursue with an integrated ERP system to gain more control over demand fluctuations, while improving vendor and customer relation management; cost-effectiveness; and a higher probability of success in business strategies.

Three ERP solutions were short-listed: COTS (Commercial Off the Shelf) solution provided by a major manufacturer, Open Source solution, and an in-house created solution.

This study uses a case study strategy, in a qualitative research mode, based on secondary research data. Taking limited access to system users into consideration as a limitation, conducting secondary research provides tools suitable for exploring a complex and subjective research phenomenon. In information systems, case study research is the most popular qualitative research method, and in particular it is well suited to understanding the effect of information technology-related innovations on organisational contexts (Darke et al.,1998).

To facilitate standard comparison among the short-listed ERP solutions and to avoid unconscious bias towards specific product brands, the following assumptions are made:

1. Three ERP solutions are short-listed after meeting two minimum requirements:
    - User-friendliness
    - Fulfilling mandatory system features based on Acme's current operating environment
2. Risk assessment is conducted based on concepts of "COTS", "Open Source" and In-house" rather than specific product brands (e.g. SAP, Linux).

Aim of the Report

Identifying Risks of the Solutions:

- Scheduling Risks: How could the solution take more time than expected
- Financial Risks: How could the solution cost more money than planned
- Security Risks: How could the solution lead to data breaches of the company
- Performance Risks: How could the solution fail to meet requirements

- User Risks: How could user action impact the system

Report Mode:
Qualitative risk assessment based on severity of risk vs likelihood of risk occurring. Lack of access to numerical data makes quantitative assessment difficult.

Disaster Recovery Solution:

- RPO of 15 minutes requires very frequent backups, and RTO of 4 hours allows for relatively slow loading of backup data
    - Differential backups every 10 minutes, these are quick to save but slow to load
    - Full backups daily, second layer of protection against data loss

- Data Sources for Risk Management Report
    - Case studies
    - Software Manufacturer Data Sheets
    - Research reports

Tools and Methods

At all times, the system must uphold its Confidentiality, Integrity and Accessibility. By implementing a new process to help circumvent the issues the company is facing, it is necessary to ensure that the system's CIA is exposed to minimal risk.

Risk process standards are a vital tool to help understand and analyse the underlying risks. One such framework that is globally accepted as an industry standard, is the SP 800-30 from the NIST. This standard is especially helpful to evaluate and convey IT risks in a concise language for business leadership to make informed decisions (Peacock, N.D.).

To assess the risks for each option and to decide upon the best approach, the report will use theories and practices as recommended by the SP 800-30. The individual steps are (NIST, 2012: 23):

1. Identifying Threat Sources and Events
2. Identifying Vulnerabilities and Predisposing Conditions
3. Determining Likelihood of Occurrence
4. Determining Magnitude of Impact
5. Determining Risk

Once threat and vulnerability pairs have been established and their likelihood to occur and impact to the organisation have been identified, a risk-level matrix will be created to classify each individual risk (Stoneburner et al., 2002: 24-25). The risk-levels of all three solutions can then be compared to establish the best solution for Acme manufacturing.

Project Timeline

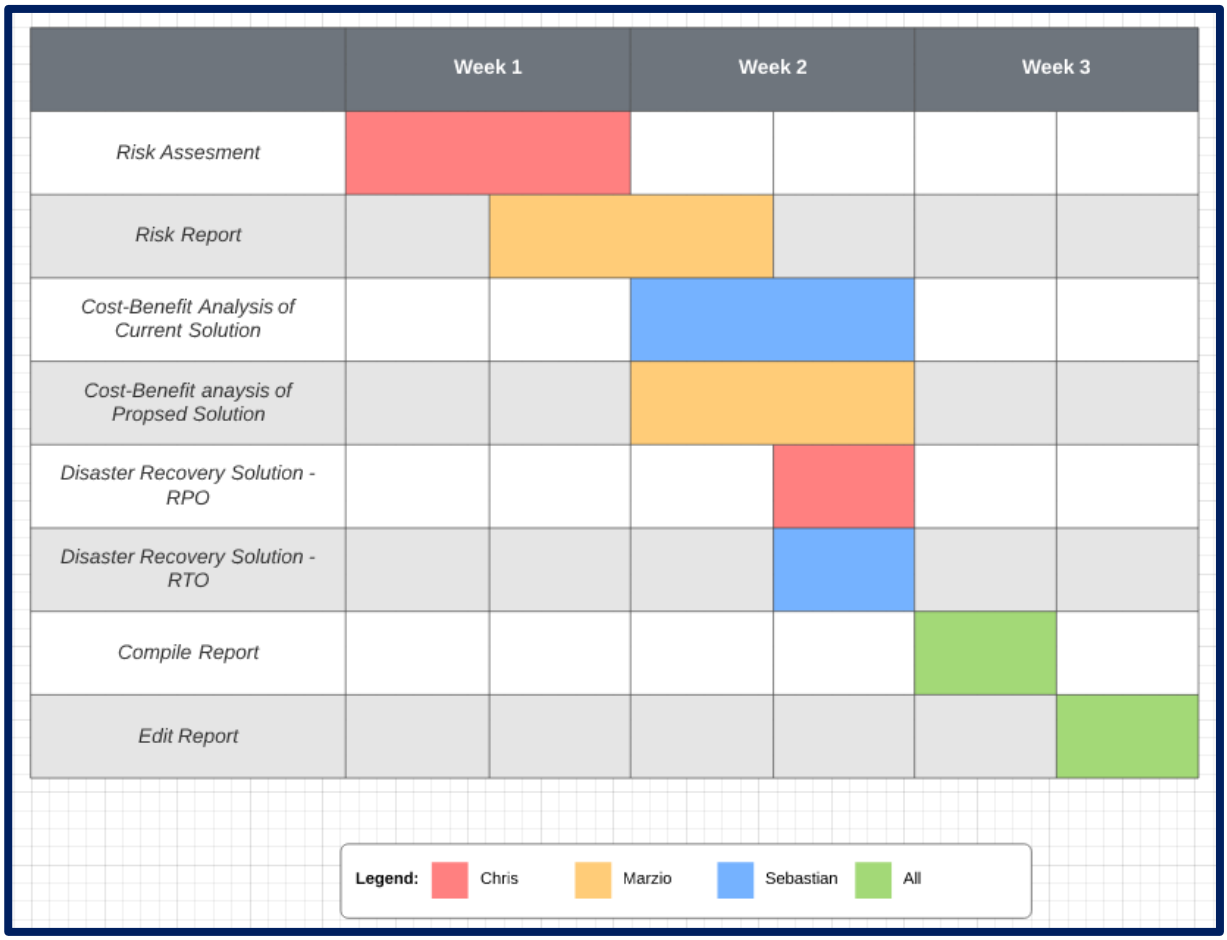

Figure 1: Gantt Chart - Risk Assessment Report Timeline

Reference List:

Darke, P., Shanks, G. & Broadbent, M. (1998) Successfully completing case study research: combining rigour, relevance and pragmatism. Information Systems Journal. 8 (4): 273-289. DOI: https://doi.org/10.1046/j.1365-2575.1998.00040.x

Irani, Z. & Love, P. (2008) Evaluating Information Systems Public and Private Sector. Oxford: Elsevier Ltd. Available from: https://www.academia.edu/2622414/Post_implementation_evaluation_of_IT_systems_A_close_review_of_practice [Accessed 3 February 2021].

NIST (2012) Guide for Conducting Risk Assessments: NIST Special Publication 800-30 Revision 1. Gaithersburg: National Institute of Standards and Technology. Available from: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf [Accessed 7. February 2021]

Peacock, J. (N.D.) What is NIST SP 800 30. Cybersaint Security. Available from: https://www.cybersaint.io/blog/what-is-nist-sp-800-30 [Accessed 7. February 2021]

Stoneburner, G. et al. (2002) Risk Management Guide for Information Technology Systems: SP 800-3. Gaithersburg: National Institute of Standards and Technology. Available from: https://dl.acm.org/doi/pdf/10.5555/2206240 [Accessed 7. February 2021]