**Development Team Project ‌**

*Risk Assessment Report ‌for‌ ‌Information Risk Management ‌(IRM)‌ ‌*

MSc‌ ‌Cyber‌ ‌Security‌ ‌

Information‌ ‌Risk‌ ‌Management,‌ ‌Unit‌ ‌6‌ ‌Submission‌ ‌

Words 1591

[**Introduction**](#_heading=h.w6cq008y16zh) **2**

[Figure 1: Solution options and estimated costs](#_heading=h.j4ab6wqlfhfl) 2

[**Threat Statement**](#_heading=h.3uosrdmf4vnm) **2**

[**Risk Assessment Approach**](#_heading=h.n3vajcq0qwqk) **3**

[**Risk Assessment Results**](#_heading=h.ky91fyz88ets) **4**

[Table 1: Solution Risk Assessment](#_heading=h.xjmp64big0a1) 4

[Figure 2: Heatmap of risks for COTS Solution](#_heading=h.43gij47xaer9) 5

[Figure 3: Heatmap of risks for Open Source Solution](#_heading=h.1gxteyklg51t) 5

[Figure 4: Heatmap of risks for Student Project Solution](#_heading=h.x0jx5nrgn04g) 6

[Figure 5: Pie Chart of Risks for COTS Solution](#_heading=h.rmbyt6wzk085) 6

[Figure 6: Pie Chart of Risks for Open Source Solution](#_heading=h.9trrkjzl3t7) 7

[Figure 7: Pie Chart of Risks for Student Project](#_heading=h.p6mjuwvmpq2g) 7

[**Risk Analysis**](#_heading=h.t60yzaqup0r) **7**

[**Cost/Benefit Analysis**](#_heading=h.a5j3nl3euh1o) **8**

[Table 2: Cost/Benefit Analysis for COTS](#_heading=h.8htdrtbzoa4i) 8

[Table 3: Cost/Benefit Analysis for Open Source](#_heading=h.pukdtsix92xk) 9

[Table 4: Cost/Benefit Analysis for Student Project](#_heading=h.m6kdk95k72xb) 9

[**System Recommendation**](#_heading=h.10xv84dk80qj) **9**

[**Disaster Recovery Solution**](#_heading=h.ihh283c2939) **10**

[Background](#_heading=h.3x29auxbbq7i) 10

[Business Scope](#_heading=h.kczrqaaxform) 10

[Solution](#_heading=h.qrdj3s9u81ik) 10

[Figure 8: Saas cloud design](#_heading=h.ubbz03lpmpmm) 11

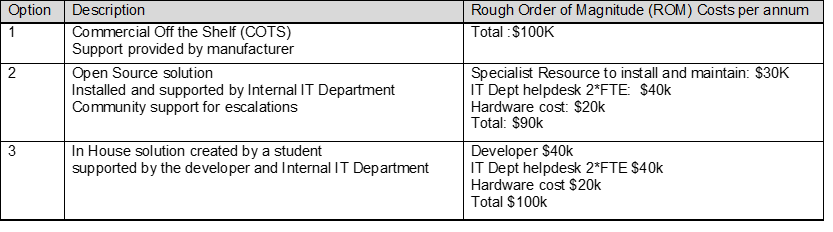
[**Summary**](#_heading=h.ivcb2ioektww) **11**

[**References**](#_heading=h.a6w0m68yutge) **12**

[**Appendix A: Custom Risk Matrix**](#_heading=h.1w9ipil0qogp) **13**

## Introduction

Acme Manufacturing is planning to introduce an Enterprise Resource Planning (ERP) solution to improve supply chain management. The company has shared three solution options in Figure 1 and these have been paired with stated or assumed solution costs. This report will recommend the option best suited to the company’s requirements, along with a corresponding disaster recovery solution that meets the given recovery objectives. The recommendations will be based on a comprehensive risk assessment that considers risks throughout the development lifecycle of each solution.



### Figure 1: Solution options and estimated costs

## Threat Statement

Whilst many threats are internal, there are also external threat actors that could pose security risks to the new system and its data (Auchard, 2018). The data assets that are attractive to attackers include:

* Business records, including financial records and supplier details
* Personal data of customers and employees
* Intellectual property

The data available can attract different threat actors, from nation state advanced persistent threats (APTs) to cyber criminals (Kerner, 2019). Whilst APTs are likely to be interested in business records and intellectual property, cyber criminals often pursue the theft of personal data to sell for profit or encrypt valuable data to charge a ransom. This system may also be targeted as it is in the supply chain of larger companies that may hold even more lucrative assets (Shackleford, 2015). Threat actor groups have varying capability levels that should be considered when determining the likelihood of a risk event (Rossebo et al., 2016). Threats to the system are not limited to external threat actors, but also include both malicious and unintentional insider threats to the system (Steffee, 2020).

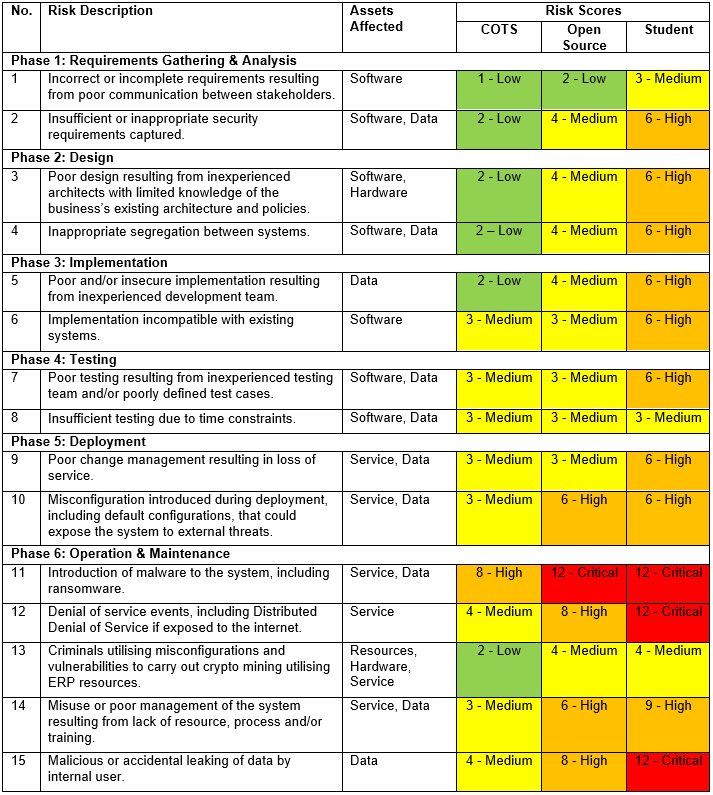
## Risk Assessment Approach

Due to lack of access to subject matter experts and users in the company, qualitative risk data has been derived from various sources specific to both the manufacturing industry and ERPs. The data from these sources have been considered in relation to the three solution options in Figure 1. The key risks have been documented in Table 1 and scored against each of the three solutions.

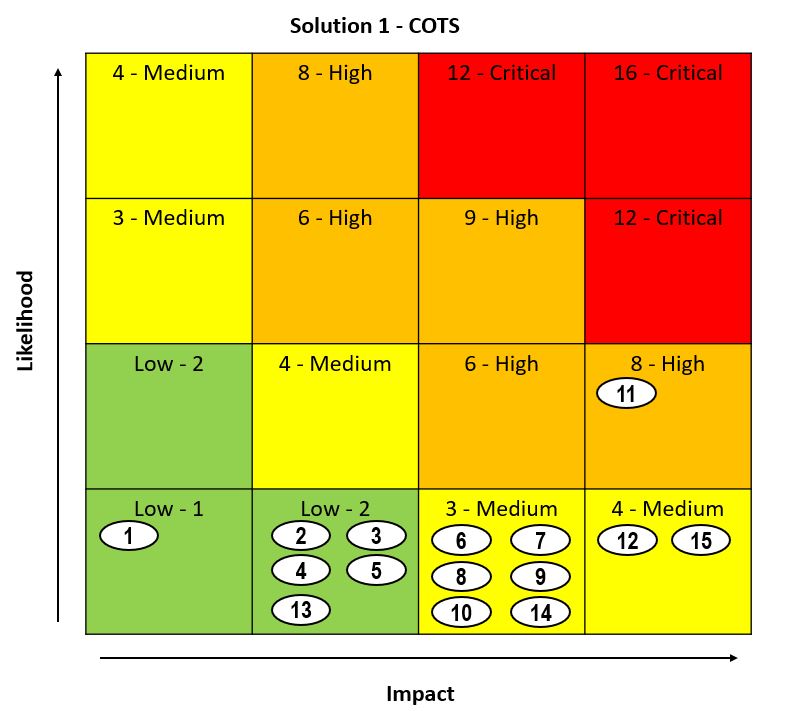
Contrary to the Design Document, a 4x4 risk matrix has been used to calculate risk scores instead of a 5x5 matrix due to the aforementioned lack of access to more granular information about Acme (Stoneburner et al., 2002). The risk scores were calculated by multiplying the estimated impact with the estimated likelihood. The impact and likelihood scores were calculated using a custom risk matrix (Appendix A). The matrix calculates the rounded average of several possible impacts (Sutton, 2014). Some impacts are calculated in a qualitative manner, such as reputational damage, and others in a semi-quantitative manner, such as financial loss. Likelihood is then calculated based on the evidence that the risk could materialise in the next 12 months. These risk scores then correspond to a rating (low, medium, high, or critical) as shown in Figures 2, 3 and 4. A mix of qualitative and semi-quantitative methods were used to calculate the risk scores in order to improve accuracy and reduce subjectivity. Without access to historic data, there are limited opportunities to employ a truly quantitative approach and in doing so this could create a false sense of security in the accuracy of the risks presented (Hubbard, 2009; Garcia, 2020).

## Risk Assessment Results

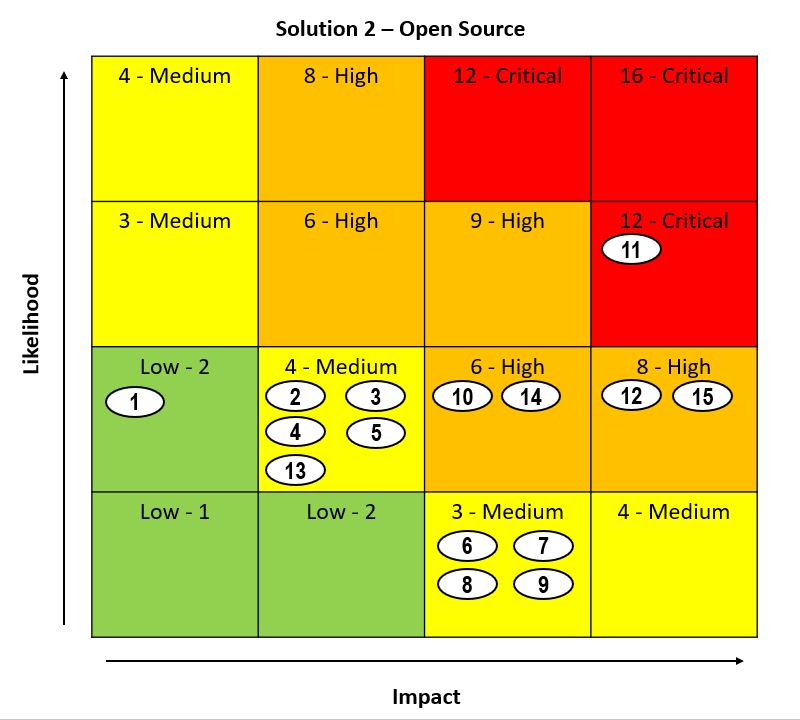
The identified risks have been split across the key development phases required to successfully implement the ERP solution. Key phases from both the software and systems development lifecycles have been included to ensure the risks to the development lifecycles of both in-house and external solutions can be considered in parallel (Hijazi et al., 2014; Kramer, 2018).



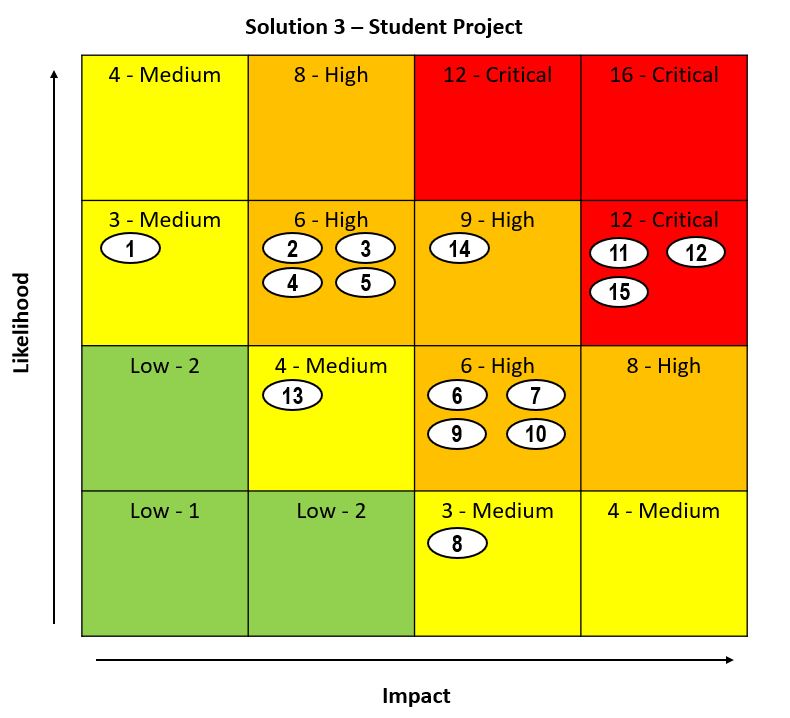
### Table 1: Solution Risk Assessment



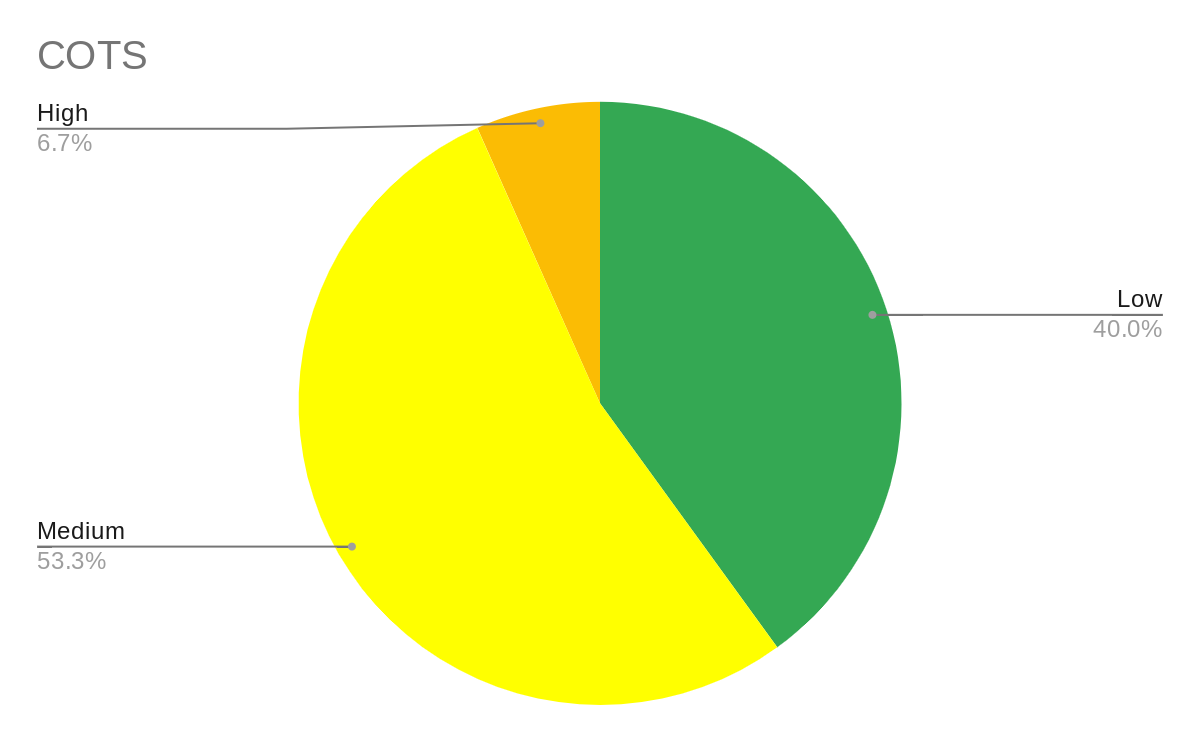
### Figure 2: Heatmap of risks for COTS Solution



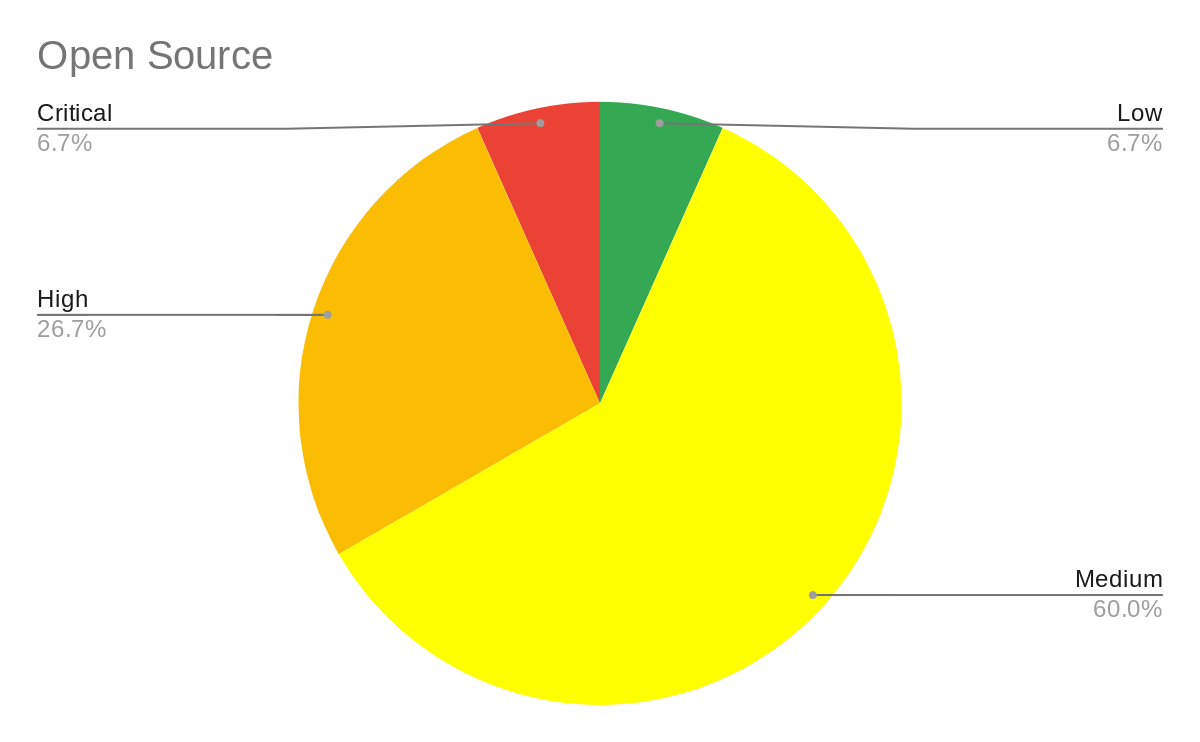
### Figure 3: Heatmap of risks for Open Source Solution



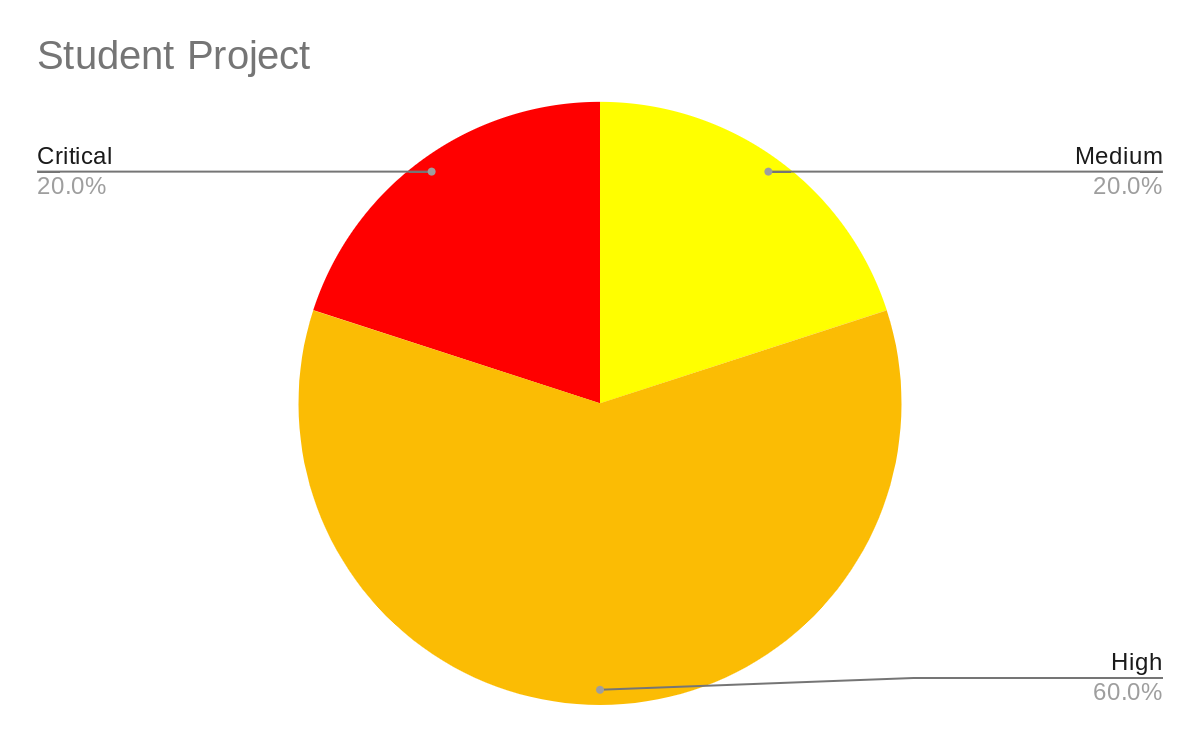
### Figure 4: Heatmap of risks for Student Project Solution



### Figure 5: Pie Chart of Risks for COTS Solution



### Figure 6: Pie Chart of Risks for Open Source Solution



### Figure 7: Pie Chart of Risks for Student Project

## Risk Analysis

Key themes have emerged from the risk scores for each solution:

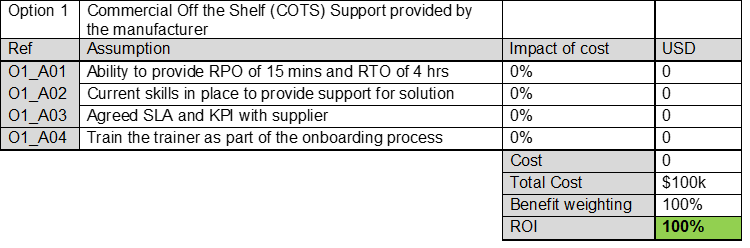
* Impacts remained consistent for all solutions against each risk, and it was likelihood that determined the risk levels. This is the result of all solutions presenting the same impact for each risk as they represent an ERP system with the same assets ultimately.
* The highest risk solution for the first five phases of the SDLC is the Student Project with the second highest being Open Source. This is due to the increased likelihood of encountering development challenges that come with inexperience, with the student being assumed to have the least experience (Roy et al., 2015). In addition, the student could represent a single point of failure for key knowledge.
* Risk scores did not surpass 12 due to the perceived value of the system and the fact that there is currently a solution in place, despite it being deemed not fit for purpose.
* Highest risks are found in the final and constant phase of the SDLC. At this point, the impacts of events will be greater as the system will be in production and the confidentiality, integrity and availability of system data is required to maintain operations and prevent damage to physical equipment (Elhabashy et al., 2019).

## Cost/Benefit Analysis

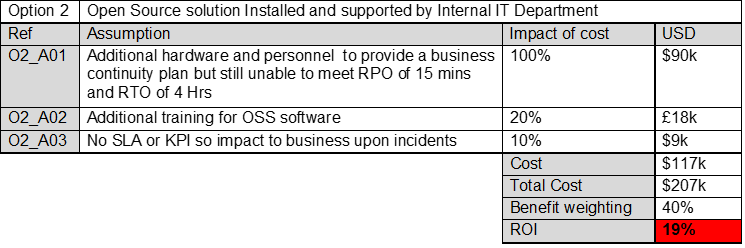
This report has utilised the Return Of Investment (ROI) equation to work out the cost benefit ratio of each solution R=(B/C)\*100. R is the ROI, B the benefits, C the costs and then the result multiplied by 100 to give a percentage for ROI. The higher the ROI percentage the higher the suitability of the proposed solution to the business requirements. The benefit is a weighted score that has been worked out as a percentage of how much the proposed solution met the business needs. If the solution met the business requirements fully it had a benefit of 100%.

A RAID (Risks, Assumptions, Issues and Dependencies) table for each solution has been created and can be found [here](https://freya247.github.io/M3_artefacts.html).

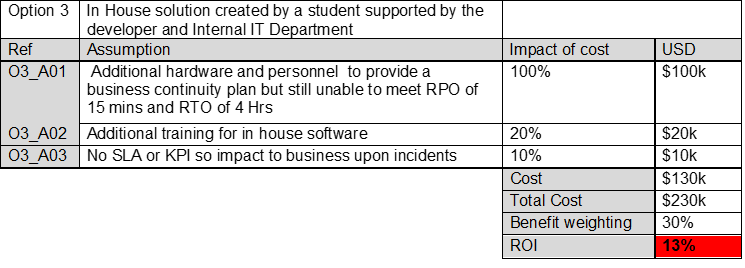
A high-level overview of the main assumptions is shown in the tables below with the ROI percentage against it.



### Table 2: Cost/Benefit Analysis for COTS



### Table 3: Cost/Benefit Analysis for Open Source



### Table 4: Cost/Benefit Analysis for Student Project

## System Recommendation

The risk assessment and cost-benefit analysis for each of the three options show a clear leader in the COTS solution. The risk assessment heatmap shows the COTS mainly in the low and medium range, whereas the other two options were mainly spread across the medium, high and critical levels. The cost-benefit analysis, utilising the weighted specification of how closely the solution met the business requirement, again clearly shows option one as the lead contender. Taking the risk assessments and cost-benefit analysis into consideration, this report's recommendation is that the COTS option is adopted for use

Whilst the inherent risks have been used to determine this recommendation, the control environment should be reviewed to ensure the residual risk is identified (Arora et al., 2004). The residual risk should drive decision making as it is a more accurate reflection of the risk environment. If a risk appetite is defined for the business, this could be used to determine which risk scores would be deemed as unacceptable and guide risk treatment decisions accordingly.

## Disaster Recovery Solution

### Background

Similar to the ERP solution, the more secure and resilient the disaster recovery (DR) solution, the more expensive it will be. Therefore all options have been examined against the criteria of risk, cost and meeting the business needs.

#### Business Scope

Functional requirements

* ERP platform for 150 staff.
* Flexibility to manage changes in supply chain and production demand.

Non-Functional requirements

* RPO of 15 mins.
* RTO of 4 hours.

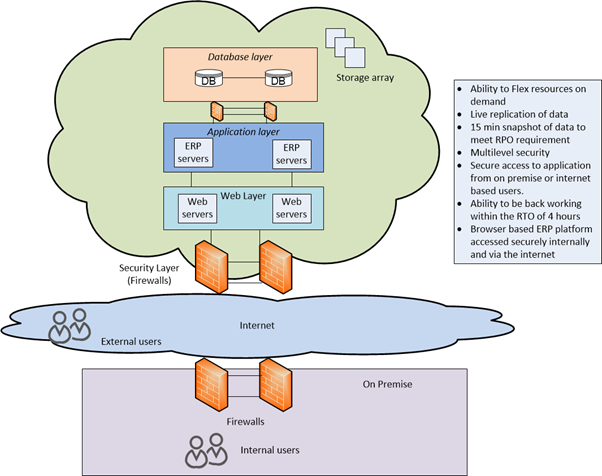
### Solution

A detailed breakdown of all three ERP solutions and their DR plans along with the rationale of why they are ruled out is detailed within a slide presentation [here](https://freya247.github.io/M3_artefacts.html).

Due to the risk analysis, budgetary requirements and business requirements of the recovery point objective (RPO) and recovery time objective (RTO), we recommend the COTS solution. To meet the RPO and RTO we recommend a cloud offering from the ERP provider rather than an on premise solution.The ERP provider will deliver a Software as a Service (SaaS) product that is accessible via a browser so negating the need to install any software on the 150 client devices. The data is encrypted at rest within the cloud, during transit whilst being used and no data is retained on the client device. Access to the ERP product is by Role Based Access Control (RBAC) and controlled by the internal IT department security team.

Figure 8 is a logical representation of the proposed SaaS platform utilising the cloud provider's resources. The product is cloud-based utilising a major cloud provider and taking advantage of their cost benefits of being able to scale up the resources at peak usage times without maintaining expensive resources 24/7. The cloud provider’s standard platform uptime is 99.5% which equates to a possible downtime of 3.65 hours per month (AWS, 2021). As part of the cloud offering the design is resilient via failover web, application and database servers along with security being built into the design.

The RPO is met via the 15 minute database snapshots being taken of the data and being held on a 28 day retention cycle with each snapshot being retained for twelve months. The RTO is met via the cloud providers SLA (AWS, 2021) plus the solution design of resilience and redundancy via dual servers at each layer.



### Figure 8: SaaS Cloud Design

## Summary

This report was to create a comprehensive risk assessment and cost-benefit analysis, also to recommend a solution that would meet the business requirements along with a disaster recovery plan for that solution. This has been completed utilising the risk assessment table and heatmaps to express the level of risk for each solution coupled with the ROI result from the cost-benefit analysis to show which solution option met the business requirement the most. The solution recommended was option one, the COTS solution and a solution diagram showing the DR solution has been detailed within this report.

## 

## References

Arora, A., Hall, D., Piato, C., Ramsey, D. & Telang, R. (2004) Measuring the risk-based value of IT security solutions. *IT Professional* 6(6): 35-42.

Auchard, E. (2018) Study Warns of Cyber Hacking Risk to Firms Using SAP, Oracle Management Software, *Insurance Journal* 96(15): 16.

AWS (2021) Amazon Compute Service Level Agreement. Available from: <https://aws.amazon.com/compute/sla/> [Accessed 18 August 2021].

Elhabashy, A., Wells, L. & Camelio, J. (2019) Cyber-Physical Security Research Efforts in Manufacturing – A Literature Review. *Procedia Manufacturing* 34: 921-931.

Garcia, A. (2020) Introduction to Cyber Risk Quantification with Open FAIR. Available from: <https://www.youtube.com/watch?v=Lm7LKWc0XtM> [Accessed 16 September 2021].

Hijazi, H. & Alqrainy, S. & Muaidi, H. & Khdour, T. (2014) Risk Factors in Software Development Phases. *European Scientific Journal* 10: 213-231.

Hubbard, D. (2009) *The Failure of Risk Management: Why It's Broken and How to Fix It.* 2nd Ed. Wiley.

Kerner, S. (March 11, 2019) How to Reduce ERP Security Risks. *eWeek*. Available from:<https://www.eweek.com/security/how-to-reduce-erp-security-risks/> [Accessed 11 September 2021].

Kramer, M. (2018) Best Practices in Systems Development Lifecycle: An Analyses Based on the Waterfall Model. *Review of Business & Finance Studies* 9(1): 77-84.

Rossebo, J., Fransen, F. & Luiijf, E. (2016) ‘Including threat actor capability and motivation in risk assessment for Smart GRIDs’, *Joint Workshop on Cyber-Physical Security and Resilience in Smart Grids*. Vienna, Austria, 12 April. IEEE. 1-7.

Roy, B., Dasgupta, R. & Chaki, N. (2015) A Study on Software Risk Management Strategies and Mapping with SDLC. *Advances in Intelligent Systems and Computing* 1(1): 121-138.

Shackleford, D. (2015) Combating Cyber Risks in the Supply Chain. Available from:<https://www.raytheon.com/sites/default/files/capabilities/rtnwcm/groups/cyber/documents/content/rtn_273005.pdf> [Accessed 11 September 2021].

Steffee, S. (2020) Insider Threats Put Data At Risk. *Internal Auditor* 77(2): 11–13.

Stoneburner, G., Goguen, A. & Feringa, A. (2002) *SP 800-30: Risk Management Guide for Information Technology Systems.* Gaithersburg, MD, USA: National Institute of Standards & Technology.

Sutton, D. (2014) *Information Risk Management.* 1st ed. Swindon, UK: BCS Learning & Development Limited.

## 

## Appendix A: Custom Risk Matrix

The following example shows Risk 9 for the Student Project solution. There is a copy of this custom matrix and an evaluation of its effectiveness [here](https://freya247.github.io/M3_artefacts.html).

