2021

Risk Assessment: Acme Manufacturing

GROUP 2
SHOTA KAMEYAMA
MUHAMMAD NASIM AKBARY
MATHEW VAN BEEK
NILS LINHOFF

Content

Comprehensive Risk Assessment Report

Selection of Framework

Considering the limitation of contacting Acme Manufacturing (AM), the qualitative risk analysis is not an option, and the quantitative risk analysis is the approach we proceed with. Please see the bulleted list of frameworks selected and passed over with justification.

- Selected
    - Open Factor Analysis for Information Risk (FAIR)
        - Quantitative Approach
        - Flexibility to go deeper layers of granularity when necessary and to enhance the visibility of risk factors and enabling troubleshoot analysis (TOG, 2016)
        - Applicable to non-information risk analysis such as project management, finance, legal risk analysis (TOG, 2021).
        - Flexibility to harmonise with other frameworks: NIST Cybersecurity Framework (NCF) as security controls (TOG, 2016) and ISO 27005 as the tool to manage risks (TOG, 2010), although they are not part of the scope.
- Not selected: qualitative approach
    - CMU Octave
    - NCF
    - ISO 27005

Open FAIR flexibility benefits analysis against business and technical risks that this report should cover. Considering these benefits, the constraints and harmonisation with other frameworks, we selected Open FAIR for risk assessment.

Risk Analysis

Open FAIR quantifies and analyses risks by breaking down into Loss Event Frequency (LEF) and Loss Magnitude (LM). LEF is the probability of the loss scenario happening during the given timeframe, while LM is the total economic significance lost when a loss event arises (TOG, 2021).

Risk Analysis Summary Table and Risk Score

Table 1-3 illustrates the summary of the LEF and LM sort by risk, including the rationale and formula of risk calculation, and Table 4 describes the risk score based on the LEF and LM sort by solution coloured by impact and probability. Details and rationale of each risk break-down analysis are illustrated in Appendix.

Risk	Solution	Loss Event Frequency	Loss Event Frequency Components			
			Explanation	Threat Event Frequency	Contact Frequency	Possibility of Action	Vulnerability
Cyber Security Attack	All	65%	- Security Breaches or Attack against medium size enterprise in the last 12 months (DDCMS, 2021)	n.a.	n.a.	n.a.	n.a.
Failure of ROI	COTS	62%	- Failure to realize the benefits of ERP @ 62% (Kiran & Reddy, 2019) - Benefit Realisation event once a year	100%	1 / year	100%	62%
	Open-Source	61.1% ≦ 76.6%	- Poor Planning @76.7% (Ebad, 2018) - Lack of IT experts @ 61.1% (Ebad, 2018)	76.7%	n.a.	n.a.	61.1%
	In-House	61.1% ≦ 76.6%	- Poor Planning @76.7% (Ebad, 2018) - Lack of IT experts @ 61.1% (Ebad, 2018)	76.7%	n.a.	n.a.	61.1%
Failure / Delay to Launch	Open-Source	61.1% ≦ 76.6%	- Poor Planning @76.7% (Ebad, 2018) - Lack of IT experts @ 61.1% (Ebad, 2018)	76.7%	n.a.	n.a.	61.1%
	In-House	61.1% ≦ 76.6%	- Poor Planning @76.7% (Ebad, 2018) - Lack of IT experts @ 61.1% (Ebad, 2018)	76.7%	n.a.	n.a.	61.1%
Termination of Community Support	Open-Source	1st yr: 60%-70% 2nd yr: 76%-89% 3rd yr: 85%-94%	- Ratio of open source project become dormant (Valiev, 2021)	n.a.	n.a.	n.a.	n.a.

100k >; 50% ≧
100k ≦; 75% ≧
250k ≦; 90% ≧
500k ≦; 90% <
1000k ≦; 100%

Table 1: LEF and its components

Risk	Solution	Loss Magnitude	Loss Magnitude Explanation	
			Formula	Rationale
Cyber Security Attack	All	$33.4k (£25.2)	$33.4k (£25.2)	- Mean direct/indirect cost that lost data or assets (DDCMS, 2021)
Failure of ROI	COTS	$350k	3 * ($100k) + $50k p.a.	- 3 times of budget (Hustad & Olsen, 2014)
	Open-Source	$50k ≦ $100k	3 * ($100/6 ($16.7k) ≦ $100/3 ($33.3k))	- 3 times of budget (Hustad & Olsen, 2014) - one sixth to one third of proprietary ERP (=COTS) implemenatation cost (Olson et al., 2018)
	In-House	$1605k	3 * $535k	- 3 times of budget (Hustad & Olsen, 2014) - Cost of ERP build from Scratch (Musienko, 2021)
Failure / Delay to Launch	Open-Source	$8634.9k ≦ $8651.5k + α	($100/6 ($16.7k) ≦ $100/3 ($33.3k)) + 8618.2k (134.24 * 8 * (251 working days - 9 holidays -28 annual leaves) * 150 staff * 25%) + lose competitive advantage (probability @ 32%)	- one sixth to one third of proprietary ERP (=COTS) implemenatation cost (Olson et al., 2018) - Revenue of Manufacturing (Alhazmi & Malaiya, 2013) - expected productivity increase (25%) loss (Kabir,2020) - lose competitive advantage (probability @ 32%) (DBEIS, 2020)
	In-House	$9153.2 + α	$535k + 8618.2k (134.24 * 8 * (251 working days - 9 holidays -28 annual leaves) * 150 staff * 25%) + lose competitive advantage (probability @ 32%)	- Cost of ERP build from Scratch (Musienko, 2021) - Revenue of Manufacturing (Alhazmi & Malaiya, 2013) - expected productivity increase (25%) loss (Kabir,2020) - lose competitive advantage (probability @ 32%) (DBEIS, 2020)
Termination of Community Support	Open-Source	$16.7k ≦ $33.3k	$100/6 ($16.7k) ≦ $100/3 ($33.3k)	- one sixth to one third of proprietary ERP (=COTS) implemenatation cost (Olson et al., 2018)

100k >; 50% ≧
100k ≦; 75% ≧
250k ≦; 90% ≧
500k ≦; 90% <
1000k ≦; 100%

Table 2: LM with formulas and rationale

Risk	Solution	Loss Magnitude	Los Magnitude Components	
			Primary Loss Magnitude	Secondary Loss Magnitude
Cyber Security Attack	All	$33.4k (£25.2)	Reponse $33.4k (£25.2)	Reputation
Failure of ROI	COTS	$350k	Productivity, Response	Competitive Advantage
	Open-Source	$50k ≦ $100k	Productivity, Response	Competitive Advantage
	In-House	$1605k	Productivity, Response	Competitive Advantage
Failure / Delay to Launch	Open-Source	$8634.9k ≦ $8651.5k + α	Productivity, Response, Replace: ($100/6 ($16.7k) ≦ $100/3 ($33.3k)) + 8618.2k	lose competitive advantage (probability @ 32%)
	In-House	$9153.2 + α	Productivity, Response, Replace: $535k + 8618.2k	lose competitive advantage (probability @ 32%)
Termination of Community Support	Open-Source	$16.7k ≦ $33.3k	Reponse, Replace $100/6 ($16.7k) ≦ $100/3 ($33.3k)	Competitive Advantage

100k >; 50% ≧
100k ≦; 75% ≧
250k ≦; 90% ≧
500k ≦; 90% <
1000k ≦; 100%

Table 3: LM components

Solution	Risk	Risk Score	Formula = Loss Event Frequency * Loss Magnitude	Loss Event Frequency	Loss Magnitude
COTS	Cyber Security Attack	$21.7k	$33.4k (£25.2) * 65%	65%	$33.4k (£25.2)
	Failure of ROI	$217k	3 * ($100k) + $50k p.a. * 62%	62%	$350k
Open-Source	Cyber Security Attack	$21.7k	$33.4k (£25.2) * 65%	65%	$33.4k (£25.2)
	Termination of Community Support	10k ≦ 31k	($16.7k ≦ $33.3k) * (60% ≦ 94%)	1st yr: 60%-70% 2nd yr: 76%-89% 3rd yr: 85%-94%	$16.7k ≦ $33.3k
	Failure of ROI	$30.6k ≦ $76.5	3 * ($16.7k ≦ $33.3k) * (61.1% ≦ 76.6%)	61.1% ≦ 76.6%	$50k ≦ $100k
	Failure / Delay to Launch	$5275.9k ≦ $6627k + α	($8634.9k ≦ $8651.5k + α) * (61.1% ≦ 76.6%)	61.1% ≦ 76.6%	$8634.9k ≦ $8651.5k + α
In-House	Cyber Security Attack	$21.7k	$33.4k (£25.2) * 65%	65%	$33.4k (£25.2)
	Failure of ROI	$980.7k ≦ $1229.4k	3 * 535k * (61.1% ≦ 76.6%)	61.1% ≦ 76.6%	$1605k
	Failure / Delay to Launch	$5592.6k ≦ $7011.4k + α	($8618.2k + α)* (61.1% ≦ 76.6%)	61.1% ≦ 76.6%	$9153.2 + α

100k >; 50% ≧
100k ≦; 75% ≧
250k ≦; 90% ≧
500k ≦; 90% <
1000k ≦; 100%

Table 4: Risk Score analysis

Risk Response Recommendation

As Open FAIR breaks down the risk items into pieces to comprehensively understand the risk, most risk response approaches are either against LEF or LM and they are either mitigated or avoided except transferable risks such as cybersecurity breach risk. Please see further details of risk response against each risk below at Table 5. We strongly recommend to plan properly and narrow the implementation scope against critical risk items to ensure implement ERP successfully. Further details are illustrated in Appendix. Also as TOG (2010; 2016) recommended, it is also recommended to incorporate NCF and ISO 27005 to manage and control security risks.

Solution	Risk	Total Risk Score	Risk Score	Risk Response Recommendation	Justification
COTS	Cyber Security Attack	$238.7k	$21.7k	- Transfer to the vendor and ensure the legal contracts to incorporate - Transfer to Cyber Insurance	- Security should be taken care by the vendor - 43% of businesses take some form of cyber insurance (DDCMS, 2021)
	Failure of ROI		$217k	- Avoid and Mitigate by proper planning by hiring project manager	- Reduce the probability to occur against LEF factors
Open-Source	Cyber Security Attack	$5338.2k ≦ $6756.2k + α	$21.7k	- Avoid or mitigate by ensuring security by hiring security staff - Avoid or mitigate by conduct security risk assesment, or ask third party to conduct vulnerability and penetration testing. - Transfer to Cyber Insurance	- Require professional skill. Hence, hire the security professionals or ask a third party to conduct security assessment to mitigate. - 43% of businesses take some form of cyber insurance (DDCMS, 2021)
	Termination of Community Support		10k ≦ 31k	- Avoid and Mitigate by contributing to the OS	- Increasing the number of commits and contributors from the company is the most effective way to mitigate the dormant risk (Valiev, 2021)
	Failure of ROI		$30.6k ≦ $76.5	- Avoid and Mitigate by proper planning especially hiring a project manager or IT professionals	- Reduce the probability to occur against LEF factors
	Failure / Delay to Launch		$5275.9k ≦ $6627k + α	- Avoid and Mitigate by proper planning especially hiring a project manager or IT professionals - Avoid and Mitigate by narrowing down the scope	- Reduce the probability to occur against LEF factors - Ensure the deployment by narrowing the scope and try implementing minimum viable product
In-House	Cyber Security Attack	$6268.1k ≦ 7852.6k + α	$21.7k	- Avoid or mitigate by ensuring security by hiring security staff - Avoid or mitigate by conduct security risk assesment, or ask third party to conduct vulnerability and penetration testing. - Transfer to Cyber Insurance	- Require professional skill. Hence, hire the security professionals or ask a third party to conduct security assessment to mitigate. - 43% of businesses take some form of cyber insurance (DDCMS, 2021)
	Failure of ROI		$980.7k ≦ $1229.4k	- Avoid and Mitigate by proper planning especially hiring a project manager or IT professionals	- Reduce the probability to occur against LEF factors
	Failure / Delay to Launch		$5592.6k ≦ $7011.4k + α	- Avoid and Mitigate by proper planning especially hiring a project manager or IT professionals - Avoid and Mitigate by narrowing down the scope	- Reduce the probability to occur against LEF factors - Ensure the deployment by narrowing the scope and try implementing minimum viable product

100k >; 50% ≧
100k ≦; 75% ≧
250k ≦; 90% ≧
500k ≦; 90% <
1000k ≦; 100%

Table 5: Risk Response Recommendation and justification

Cost-Benefit Analysis

The cost-benefit analysis starts calculating the risk response cost suggested in Table 5. Table 6 illustrates the rationale of implementation cost and maintenance cost, including the risk response cost, assuming that all of the risks mentioned are avoidable (which is the limitation of this study) by conducting risk response practices. As the numerical benefit is the same in all three solutions, productivity increases by 25%, the comparison focuses on each cost. Each cost includes implementation or maintenance cost and risk response cost. Risk response costs mainly include human resource costs such as an experienced project manager, cyber security officer, and IT support staff referenced UK National Career Service (N.D.), a cyber insurance cost at $0.4k (Get Indemnity, 2021), and penetration test cost at $150k-$300k (Glover, 2021). As Table 6 illustrates, the COTS solution is more beneficial in both implementation and maintenance, as OS and IH solutions require more professional staff to maintain the system to avoid risks.

Solution	Cost				Benefit
	Implementation + Risk Response	Rationale	Maintenance + Risk Response	Rationale	
COTS	$243.1k < $293.1k	= $100k + $50k + 0.4k + (50k) + 92.7k - COTS implementaion @ $100k - COTS support @ $50k - a cyber security officer @ $50k per year (National Career Service, N.D.) - cyber insurance $0.4k / year (Get Indemnity, 2021) - an experienced project manager @ $92.7k/year (National Career Service, N.D.)	$50.4 < $100.4	= $50k + ($50) + 0.4 - COTS support @ $50k (- a cyber security officer @ $50k per year (National Career Service, N.D.)) - cyber insurance $0.4k / year (Get Indemnity, 2021)	$8618.2k
Open-Source	$284.5k < $324.5k	= $25k < 50k +0.4k + 50k + 15k-30k + 33.8k*3 + 92.7k - OS Implementation @ (COTS)/6 - (COTS)/3 = $25k < $50k (Olson et al., 2018) - a cyber security officer @ $50k per year (National Career Service, N.D.) - 15k-30k / time for a penetration testing (Glover, 2021) - cyber insurance $0.4k / year (Get Indemnity, 2021) - an experienced project manager @ $92.7k/year (National Career Service, N.D.) - three IT support staff @ 33.8k * 3 / year (National Career Service, N.D.)	$259.5k < $274.5k	= 0.4k + 50k + 15k-30k + 33.8k*3 + 92.7k - a cyber security officer @ $50k per year (National Career Service, N.D.) - 15k-30k / time for a penetration testing (Glover, 2021) - cyber insurance $0.4k / year (Get Indemnity, 2021) - an experienced project manager @ $92.7k/year (National Career Service, N.D.) - three IT support staff @ 33.8k * 3 / year (National Career Service, N.D.)	
In-House	$794.5k < $800.9k	= $535k +0.4k + 50k + 15k-30k +0.4k + 33.8k*3 + 92.7k - IH Implementation @ $535k (Musienko, 2021) - a cyber security officer @ $50k per year (National Career Service, N.D.) - 15k-30k / time for a penetration testing (Glover, 2021) - cyber insurance $0.4k / year (Get Indemnity, 2021) - an experienced project manager @ $92.7k/year (National Career Service, N.D.) - three IT support staff @ 33.8k * 3 / year (National Career Service, N.D.)	$259.5k < $274.5k	= 0.4k + 50k + 15k-30k + 33.8k*3 + 92.7k - a cyber security officer @ $50k per year (National Career Service, N.D.) - 15k-30k / time for a penetration testing (Glover, 2021) - cyber insurance $0.4k / year (Get Indemnity, 2021) - an experienced project manager @ $92.7k/year (National Career Service, N.D.) - three IT support staff @ 33.8k * 3 / year (National Career Service, N.D.)	

Table 6: Cost-Benefit Analysis

Recommended Solution

As illustrated in Table 7, we recommend the lowest impact item, the COTS ERP, considering the risk score. The main reason is the risk of a launch failure that is the highest risk for OS and IH solutions, which impacts the expected revenue increase by 25% and possibly to lose competitiveness in the industry at 32% of possibility (DBEIS, 2020). COTS does not have this risk because it already has the implementation package.

Solution	Recommendation	Total Risk Score Aginst Solutions	Cost		Benefit
			Implementation + Risk Response	Maintenance + Risk Response	
Commercial Off the Shelf	High	$238.7k	$243.1k < $293.1k	$50.4 < $100.4	$8618.2k
Open-Source	Low	$5338.2k ≦ $6756.2k + α	$284.5k < $324.5k	$259.5k < $274.5k	
In-House	Lowest	$6595k ≦ 8262.5k + α	$794.5k < $800.9k	$259.5k < $274.5k	

Table 7: Recommended Solution

Disaster Recovery Solution

RPO&RTO

AM stated that their business recovery goals are a recovery point objective of 15 minutes and a recovery time objective of 4 hours.

However, Cegiela (2006) classifies the ERP system as a back office system and recommends a RPO between >1h and <1day and a similar RTO as described in Figure 1.

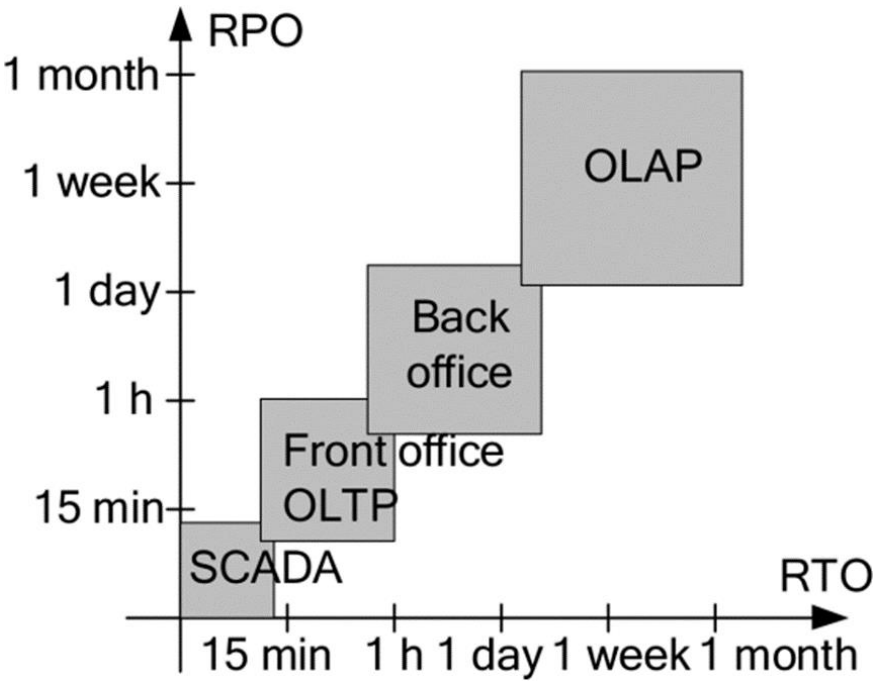

Figure 1 (Cegiela, 2006)

Since AM is using the ERP system to manage its supply chain, a shorter RPO might be more suitable for this specific industry, as Figure 2 shows the industry specific revenue loss in case of an

unavailability of an critical system. For AM the revenue loss would be $19,836 / hour (150 staff, $134,24 revenue loss in manufacturing industry/hour: 134.24 * 150 / hour). So, a 4 hour RTO will result in an approximate revenue loss of $79,344 until normal operations can continue.

Industry Sector	Revenue/ Hour	Revenue/ Employee-Hour Hour
Energy	$2,817,846	$569.20
Telecommunications	2,066,245	186.98
Manufacturing	1,610,654	134.24
Financial institutions	1,495,134	1,079.89
Information technology	1,344,461	184.03
Insurance	1,202,444	370.92
Retail	1,107,274	244.37
Pharmaceuticals	1,082,252	167.53
Banking	996,802	130.52
Food/beverage processing	804,192	153.1
Consumer products	785,719	127.98
Chemicals	704,101	194.53
Transportation	668,586	107.78
Utilities	643,250	380.94
Health care	636,030	142.58
Metals/natural resources	580,588	153.11
IT professional services	532,510	99.59
Electronics	477,366	74.48
Construction and engineering	389,601	216.18
Media	340,432	119.74
Hospitality and travel	330,654	38.62

Figure 2 Industry specific revenue loss (Alhazmi and Malaiya, 2013)

Furthermore, one of the biggest business risks to AM are natural hazards, especially extreme weather events (Crichton, 2006, as cited in Wedawatta et al., 2010), hence the need for the backup system to be located in a different region (geographical redundancy). Another risk are cybersecurity attacks, which comprise the system and even sometimes make it usable (Saleem et al., 2017; Heikkilä et al., 2016).

Taking these risks and the possible revenue loss into account a RPO of 15min and an RTO of 4h seems justified. To meet these recovery goals, we propose an active/passive model whereas the passive system is cloud based and geographical independent. An active/passive model best meets the requirements regarding initial and operational cost as well as the risk of data loss (Alhazmi and Malaiya, 2013).

Disaster Recovery Solution Design:

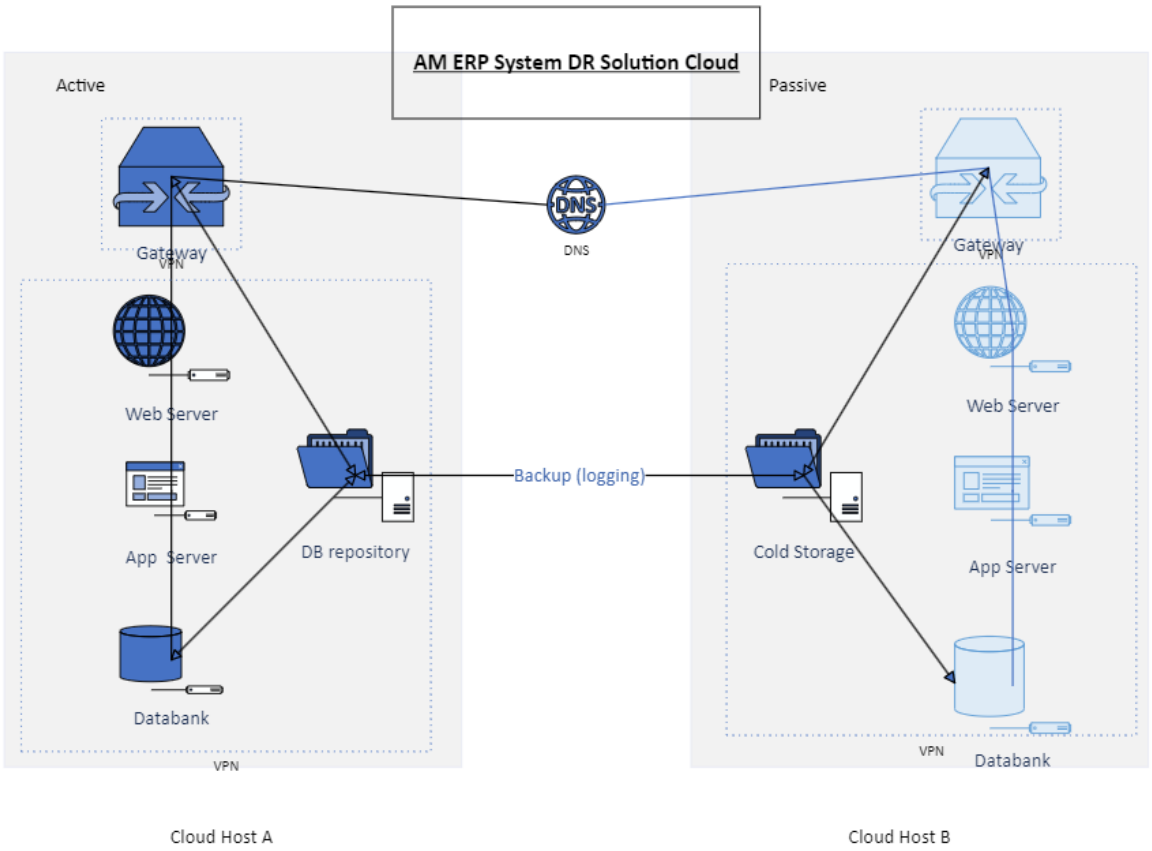

Figure 3 Active/Passive Solution

Figure 3 displays our proposed active passive solution for the ERP system which is meeting the business recovery goals. The proposed design is a warm standby which is a compromise of hot standby (low RTO, high cost) and cold standby (high RTO, low cost) (Alhazmi and Malaiya, 2013). This solution is using Microsoft Azure cloud technology for the secondary site.

The primary system is set up in a cloud environment. This can be a private cloud or a public cloud vendor such AWS, Azure or Google which supports IAAS and should be different to the secondary site. The minimum SLA for the primary site is local or zone redundancy.

Alternatively the primary system can be hosted on premise, then a secondary database, appserver and web server will be used to provide redundancy for planned outage and maintenance (see Figure 12 in Appendix for an example). However, since the cloud environment has a certain degree of redundancy built in, we recommend a cloud/cloud solution.

The active system has a database, app server, frontend, and communications via a gateway with the internet. Databases are backed up onto storage which then is synchronised with storage in a cloud system. The architecture then is mirrored in a cloud IAAS environment where the servers have all the necessary application code but are not powered up to save on computational costs. The secondary site has an SLA of geo-redundancy to ensure that an outage of the second site is not very likely. The systems are secured with a gateway, firewalls, and virtual private networks according to AM security needs.

In the case of an outage in system A system B can be powered up manually and restore the data from the latest backup. Depending on the cloud provision plan, the time to make system B functional can be well under 4h.

How the DR solution challenges have been addressed

The disaster recovery solution being discussed is an Active Passive Solution (APS), which includes a fully Azure cloud environment (also backed up to the cloud). This solution addresses various challenges pertaining resilience, network security and vendor selection in the below ways;

Resilience

- Critical services have been identified and replicated in the Azure cloud every 15 minutes, offsite cloud backup once a day. In the event of a severe disruptive incident at the primary site, the Azure cloud Infrastructure As A Service (IAAS) environment can be manually started, and the latest backup restored.
- The Azure Cloud passive site has geo-redundancy. Microsoft Azure boasts durability of data objects uptime of at least 99.99% per annum (Microsoft, 2021).
- RTO and RPO requirements have been identified and addressed in the solution.
- Processes and procedures are documented in business services.
- Roles and responsibilities are documented and assigned.
- Quarterly tabletop exercises to be performed with an annual planned DR test.

Network Security

- Using the load balancer Azure application gateway-with a firewall, offers Secure Socket Layer (SSL) encryption and decryption (Microsoft, 2021).
- Data is encrypted in transit and at rest in Azure cloud (Antonopoulos, P, et al 2020).
- Implementation of virtual private networks (VPN), with specific network traffic rules to segment the different application layers.

Vendor Selection / Lock In

- MS Azure IAAS could be transferred to another vendor such as AWS, Alibaba elastic compute service or DigitalOcean (Villamizar, M., et al 2016).

It's worthwhile mentioning that the APS solution aforementioned also addresses cost optimization in certain ways including;

- Quarterly review on computational power and use scalable options wherever possible.
- Utilization of cold storage to store the data backup, this cold blob storage from Azure offers lower storage costs however it does also incur higher access costs (Microsoft, 2021).

Disaster recovery items

Order of activation	**Disaster recovery items**	**RPO**	**RTO**
0	DB repository	-	-
1	Data bank	15m	~1h*
2	App server	-	~1h*
3	Web server	-	~1h*
4	Gateway	-	~0,5*
	Total Time	**15min**	**~3,5h***

* This is an estimate, the actual RTO depends on factors such as size and quality of code and computational tier selection

References

1. Alhazmi, O.H. & Malaiya, Y.K. (2013) 'Evaluating disaster recovery plans using the cloud', *2013 Proceedings Annual Reliability and Maintainability Symposium (RAMS)*. Orlando, FL, 28-31 January. Orlando: IEEE. 1–6. DOI:10.1109/RAMS.2013.6517700.
2. Antonopoulos, P., Arasu, A., Singh, K. D., Eguro, K., Gupta, N., Jain, R., Kaushik, R., Kodavalla, H., Kossmann, D., Ogg, N., Ramamurthy, R., Szymazek, J., Trimmer, J., Vaswani, K., Venkatesan, R. & Zwilling, M. (2020) 'Azure SQL database always encrypted', *Proceedings of the 2020 ACM SIGMOD International Conference on Management of Data.* Porland, Oregon, 14-19 June. New York: Association for Computing Machinery. 1511-1525. DOI: https://doi.org/10.1145/3318464.3386141
3. Cegiela, R. (2006) 'Selecting Technology for Disaster Recovery', *2006 International Conference on Dependability of Computer Systems*. Szklarska Poreba, 25-27 May. Szklarska:IEEE. 160–167. DOI:10.1109/DEPCOS-RELCOMEX.2006.49.
4. Department for Business, Energy & Industrial Strategy (2020) Longitudinal Small Business Survey: SME Employers (businesses with 1-249 employees) - UK, 2019. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/889656/LSBS_2019_employers.pdf [Accessed 20 November 2021].
5. Department for Digital, Culture, Media & Sport (2021) Cyber Security Breaches Survey 2021. Available from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021 [Accessed 17 December 2021].
6. Ebad, S. A. (2018) An exploratory study of ICT projects failure in emerging markets. *Journal of Global Information Technology Management.* 21(2): 139-160.
7. Get Indemnity (2021) Cyber Insurance. Available from: https://getindemnity.co.uk/business-insurance/cyber [Accessed 20 December 2021].
8. Glober, G. (2021) How Much Does a Pentest Cost? Available from: https://www.securitymetrics.com/blog/how-much-does-pentest-cost [Accessed 20 December 2021].
9. Heikkilä, M., Rättyä, A., Pieskä, S. & Jämsä, J. (2016) 'Security challenges in small-and medium-sized manufacturing enterprises', *2016 International Symposium on Small-scale Intelligent Manufacturing Systems (SIMS).* Narvik, Norway, 21-24 June. IEEE. 25-30.
10. Hustad, E. & Olsen, D. H. (2014) 'ERP Implementation in an SME: a Failure Case', in: Devos, J., Landeghe. H. & Deschoolmeester, D. (eds) *Information Systems for Small and Medium-sized Enterprises.* Berlin, Heidelberg: Springer. 213-228.

11. Kabir, M. R. (2020) Impact of ERP Implementation on Productivity and Profitability: An Empirical Study on the Largest Bangladeshi Steels Manufacturer. *International Journal of Entrepreneurial Research*. 3(4): 88-94.
12. Kiran, T. & Reddy, A. (2019) Critical success factors of ERP implementation in SMEs. *Journal of Project Management*. 4(4): 267-280. DOI: 10.5267/j.jpm.2019.6.001
13. Microsoft (2021) Data redundancy - Azure Storage | Microsoft Docs. Available from: https://docs.microsoft.com/en-us/azure/storage/common/storage-redundancy [Accessed 17 December 2021].
14. Microsoft (2021) Firewall, App Gateway for virtual networks - Azure Example Scenarios | Microsoft Docs. Available from: https://docs.microsoft.com/en-us/azure/architecture/example-scenario/gateway/firewall-application-gateway [Accessed 17 December 2021].
15. Microsoft (2021) Hot, Cool, and Archive access tiers for blob data - Azure Storage | Microsoft Docs. Available from: https://docs.microsoft.com/en-us/azure/storage/blobs/access-tiers-overview [Accessed 17 December 2021].
16. Musienko, Y. (2021) How Much Does It Cost To Develop An ERP Software. Available from: https://merehead.com/blog/much-cost-develop-erp-software/ [Accessed 17 December 2021].
17. National Careers Service (N.D.) National Careers Service. Available from: https://nationalcareers.service.gov.uk/ [Accessed 20 December 2021].
18. Olson, D. L., Johansson, B. & De Carvalho, R. A. (2018) Open source ERP business model framework. *Robotics and Computer-Integrated Manufacturing*. 50: 30-36.
19. The Open Group Standard (2010) Open FAIR – ISO/IEC 27005 Cookbook. Available from: https://publications.opengroup.org/c103 [Accessed 25 November 2021].
20. The Open Group Standard (2016) Open FAIR – NIST Cybersecurity Framework Cookbook. Available from: https://publications.opengroup.org/g167 [Accessed 10 December 2021].
21. The Open Group Standard (2021) Risk Analysis (O-RA), Version 2.0.1. Available from: https://publications.opengroup.org/standards/c20a [Accessed 25 November 2021].
22. Saleem, J., Adebisi, B., Ande, R. & Hammoudeh, M. (2017) 'A state of the art survey-Impact of cyber attacks on SME's', *Proceedings of the International Conference on Future Networks and Distributed Systems*. Cambridge, UK, 19-20 July. New York: Association for Computing Machinery. DOI: 10.1145/3102304.3109812.
23. Valiev, M. (2021) External Factors in Sustainability of Open Source Software. *Institute for Software Research School of Computer Science Carnegie Mellon University*. Available From

http://reports-archive.adm.cs.cmu.edu/anon/anon/usr/ftp/usr0/ftp/isr2021/CMU-ISR-21-103.pdf [Accessed 17 December].

24. Villamizar, M., Garces, O., Ochoa, L., Castro, H., Salamanca, L., Verano, M., Casallas, R., Gil, S., Valencia, C., Zambrano, A. & Lang, M. (2016) 'Infrastructure cost comparison of running web applications in the cloud using AWS lambda and monolithic and microservice architectures', *2016 16th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid),* Cartagena, Colombia, 16-19 May. Columbia: IEEE. 179-182. DOI: 10.1109/CCGrid.2016.37
25. Wedawatta, G., Ingirige, B. & Jones, K. (2010) 'Coping strategies against extreme weather events: A survey of SMEs in the UK', *RICS Construction and Building research conference (COBRA) 2010*. Université Paris-Dauphine, Paris, July.
26. Zawada, B. (2014) 'The practical application of ISO 22301', *Journal of Business Continuity & Emergency Planning*. 8(1): 83–90.

Appendix

Cybersecurity Attack Risk

Figure 4 illustrates cybersecurity attack risk that broke down into LEF as a possibility of security breaches against medium enterprise in the last 12 months and financial magnitude that impacts AM referenced from Department for Digital, Culture, Media & Sport (DDCMS) (2021). Against the COTS solution, AM should transfer this risk to the vendor as it is their responsibility to maintain the security or apply Cyber Insurance that 43% of business enterprises apply (DDCMS, 2021). For other solutions, it is recommended to hire security professionals to proceed with mitigation practices, and/or proceed vulnerability and penetration testing to ensure that the security vulnerabilities do not exist.

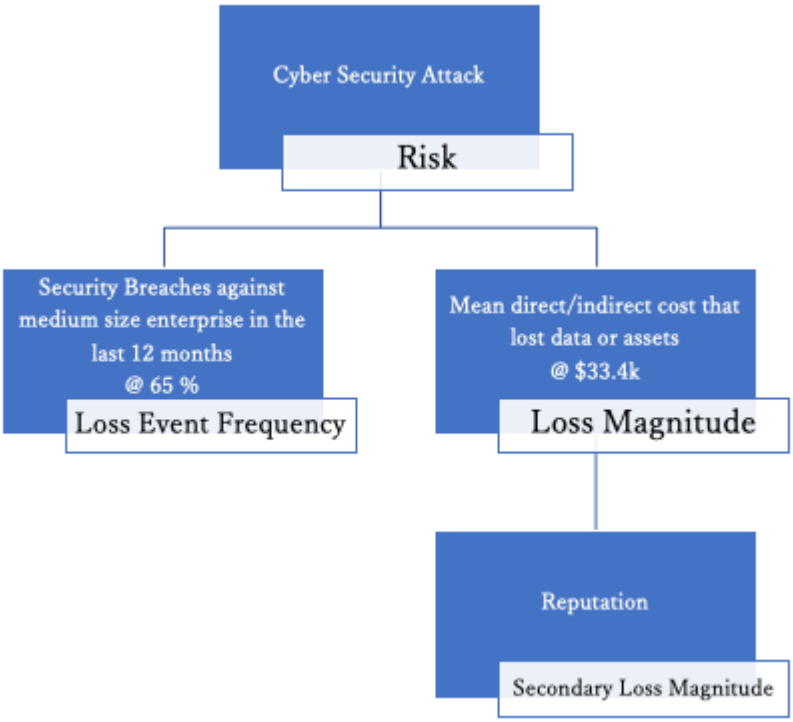

Figure 4: Cyber Security Attack Risk (All Solution)

Return on Investment (ROI) risk

LEF broke down to Threat Event Frequency (TEF) and Vulnerability (Vuln), while LM does the same to Primary Loss Magnitude (PLM) and Secondary Loss Magnitude (SLM). Open FAIR is helpful to break down when it is challenging to measure LEF or LM or consider better objective data and further details of threat events or magnitude (TOG, 2021). Figure 5-7 illustrates the risk of each solution's ROI failure. LEF consists of poor planning and a lack of IT experts that lead to ICT project failures (Ebad, 2018), which applies to the ERP project. LM is different from scenarios: 1) Commercial Off the Shelf (COTS) LM is three times of budget (Hustad & Olsen, 2014); 2) Open-Source (OS) ERP costs one-sixth to one-third of proprietary ERP implementation (Olson et al., 2018). Hence, LM of OS is the combination of three times of OS ERP cost; 3) In-House (IH) ERP costs $535k when building from scratch (Musienko, 2021). Hence the impact is the largest when applying three times of IH ERP cost. The risk responses against ROI risk is to focus more on mitigation or avoidance practices against LEF which consists of planning and incorporating IT capabilities by hiring ICT professionals, which also leads to mitigating the impact.

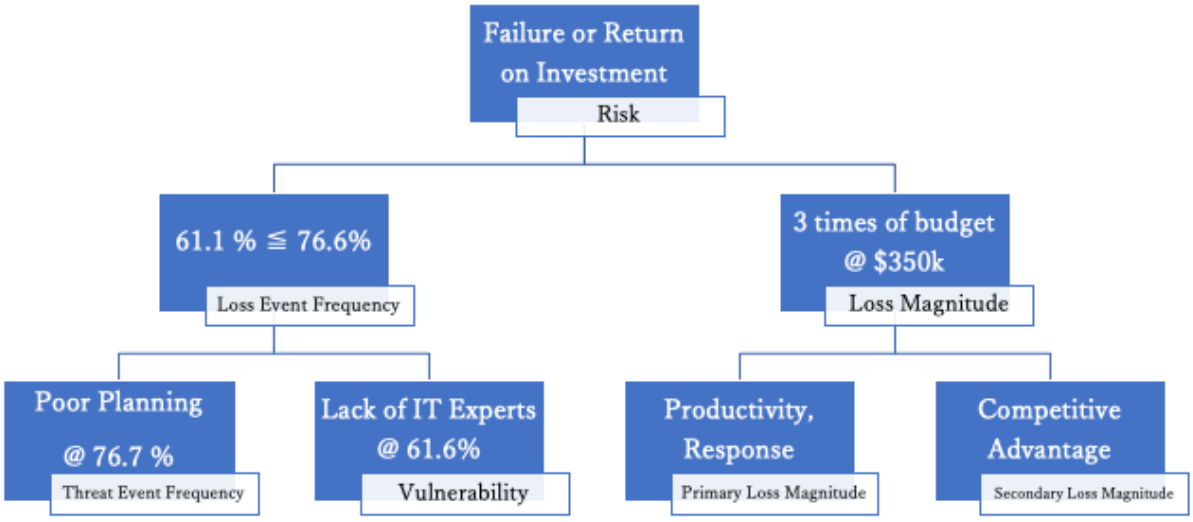

Figure 5: Failure of ROI risk (COTS)

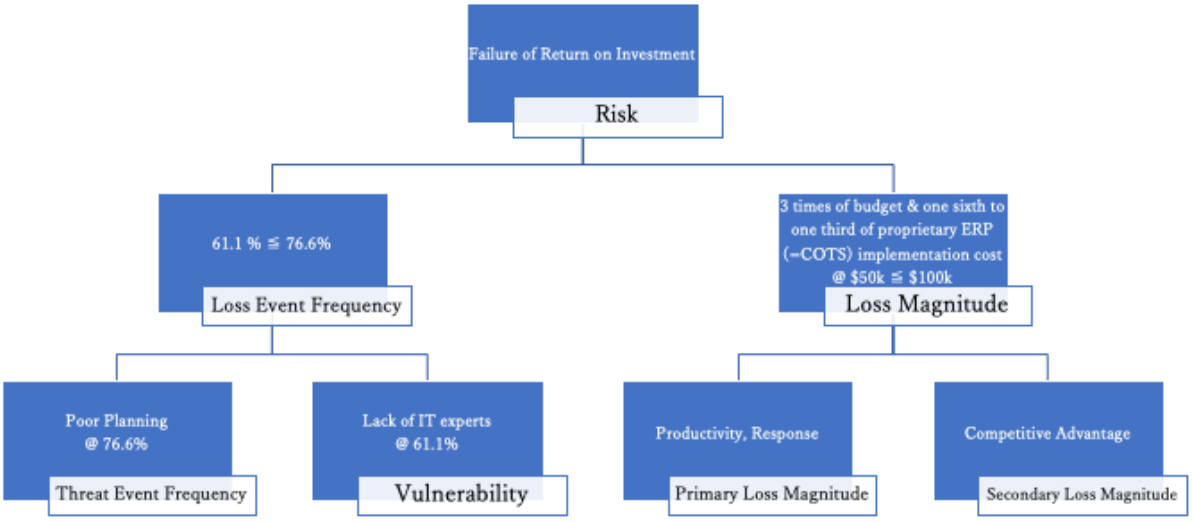

Figure 6: Failure of ROI risk (OS

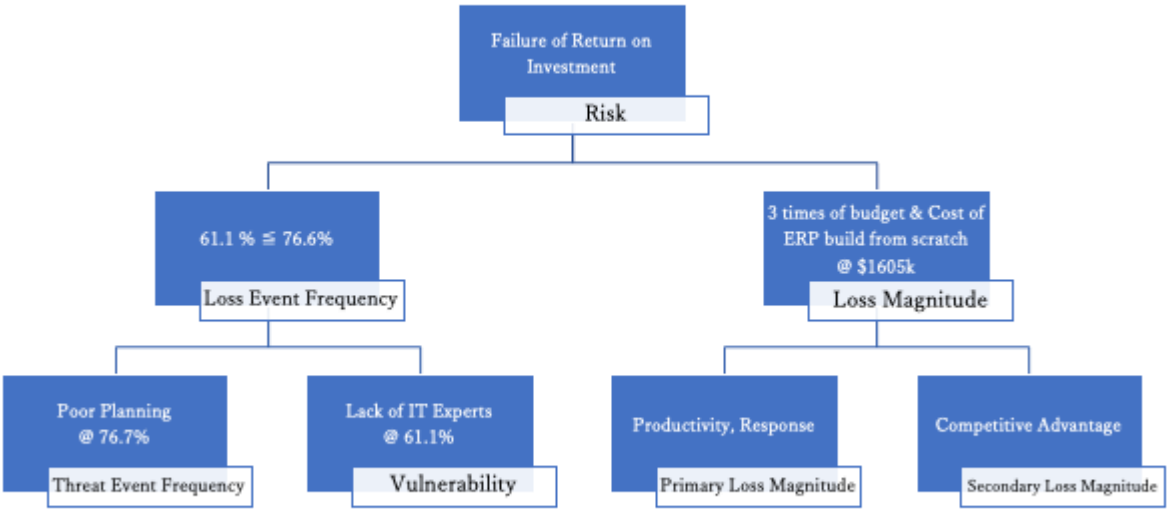

Figure 7: Failure of ROI risk (IH)

Launch Failure Risk

ERP implementation, especially OS and IH ERP, has the risk of a launch failure. Figure 8 and 9 illustrate the risk break-down structure. LEF is the same as ROI failure in figure 5-7. LM is the cost of ERP implementation, $167k ≦ $33.3k for OS ERP and $535k for IH ERP, and loss of opportunity benefit that is expected productivity increase by 25% (Kabir, 2020), which calculated industry revenue per staff illustrated in Figure 2 (Alhazmi and Malaiya, 2013) multiplied by staff members in a

year that is $8618.2k as PLM and loss of competitive advantage probability of 32 % referenced from Department for Business, Energy & Industrial Strategy (DBEIS) (2020) as SLM. Depending on the SLM impacts, the magnitude potentially becomes enormous.

The most impactful risk is the loss of expected opportunity revenue at $8618.2k. This risk should be avoided. Risk response practice against this is the same as ROI risk, focusing on reducing the probability to occur against LEF factors. In addition to the mitigation practice against LEF factors, the company should narrow down the implementation scope to make sure that the ERP implementation is successfully done.

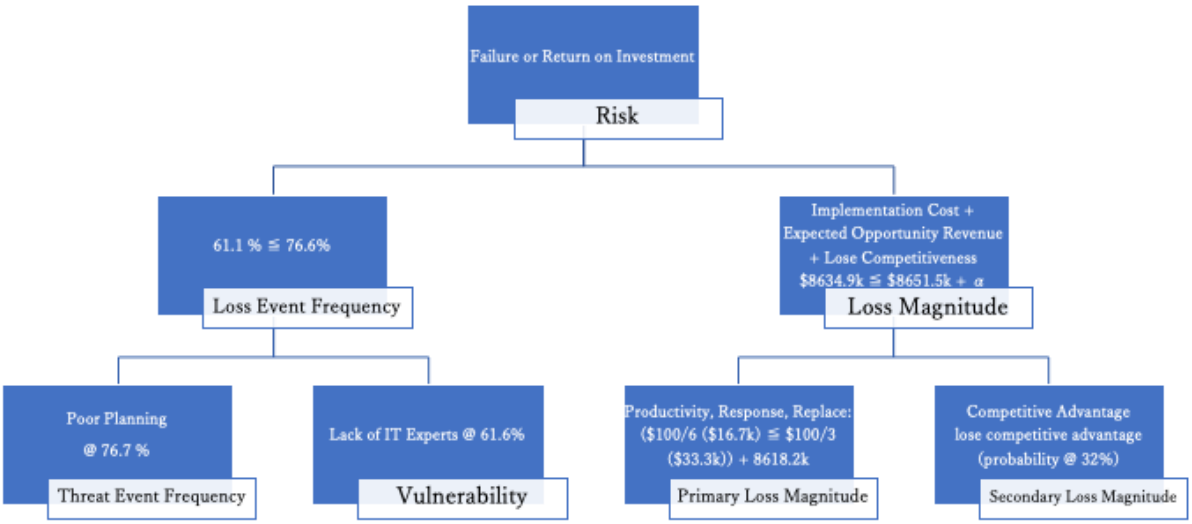

Figure 8: Failure to Launch risk (OS)

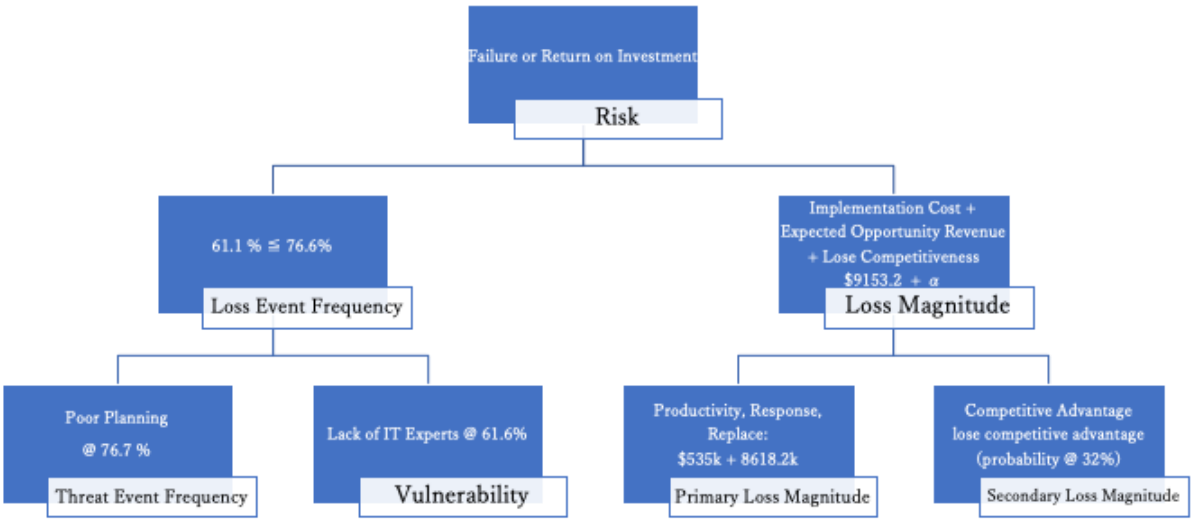

Figure 9: Failure to Launch risk (In-House)

OS Dormancy Risk

Lastly, Figure 10 illustrates the risk of termination of OS community support. Valiev (2021) conducted a quantitative survival analysis using Cox Proportional-Hazards Model. Using the model, he found the overall probability of packages survival in PyPI and npm (figure 11), which we applied to the risk

analysis because of the nature of the OS community. The OS will embrace security risks without proper maintenance and cannot update competitive features. AM needs to replace the system in the future, which will increase ICT cost enormously.

As the survival rate in the third year is 85-94%, this risk is most likely to occur. However, Valiev (2021) also demonstrated that the many more commitments and contributors involved, the more possible it is to survive. Therefore, the mitigation practice against OS Dormancy Risk is to contribute to the OS, and contribution should be the part of the AM IT professionals responsibility. This will mitigate this risk.

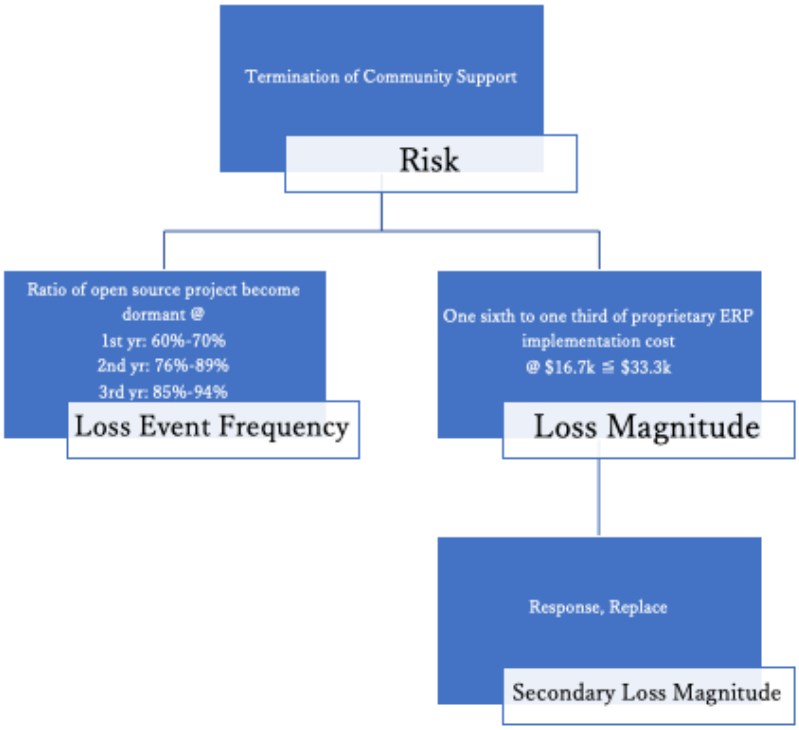

Figure 10: Termination of Community Support (OS)

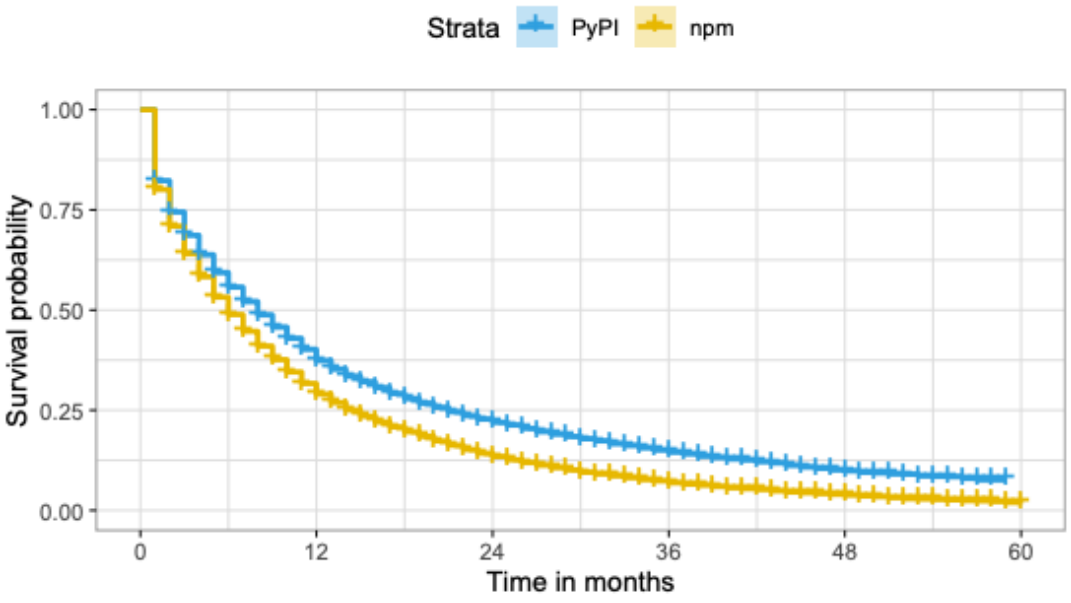

Figure 11: Overall probability of packages survival in PyPI and npm (Valiev, 2021)

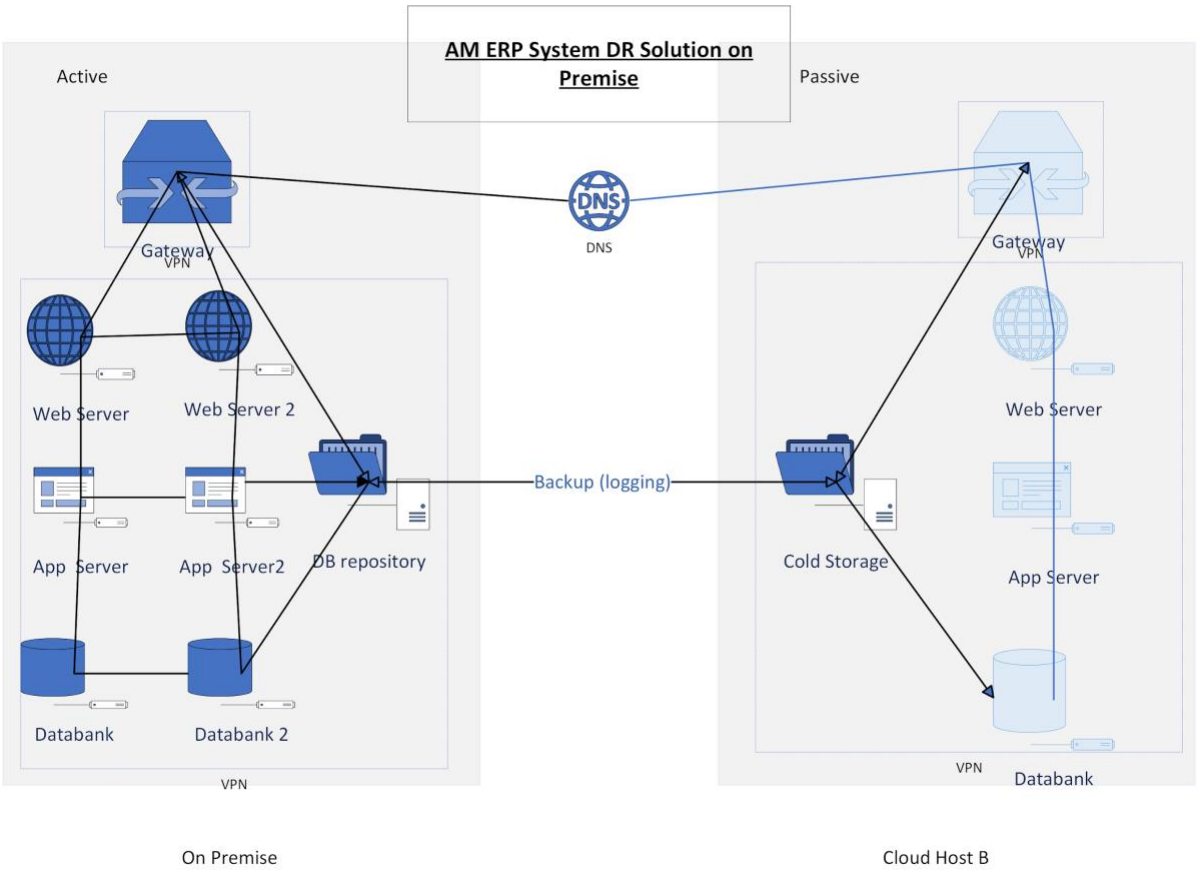

Figure 12: On Premise hosting example