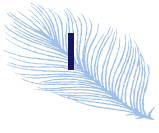
ACME Manufacturing

Risk Assessment Report

Group 2

Kingsley Onyeemeosi
Michael Geiger
Richard Meadows
Zihaad Khan

TABLE OF CONTENTS



Risk Assessment Methodology

Regarding Risk Management and Cyber Security, there are many assessment frameworks which prioritise various factors and treat them in different depths. Selecting the right framework is fundamental to an appropriate risk assessment and is therefore a prerequisite for successful risk management. The Core Unified Risk Framework (CURF) (Ulven & Wangen, 2021) represents an in-depth investigation of risk frameworks, which enables a comparison of risk assessment methods.

The study by Wangen et al. (2018) compares 11 risk assessment methodologies, which are used as a basis for deciding which framework to use. The frameworks that performed the best in the study and can be applied in relation to the risk assessment report are FAIR, ISO 27005, NIST Special Publication (SP) 800-30 and OCTAVE. Table 4 (Appendix A) summarises the results of the study from Wangen et al. (2018) in relation to these frameworks. A first comparison of the results suggests that the ISO 27005 framework addresses most factors, while OCTAVE scores the lowest. In addition, Amini & Jamail (2018) stated that OCTAVE has disadvantages in terms of complexity, documentation of requirements and characteristics, as well as in threat classification and identification.

A comparison of the NIST SP 800-30 and ISO 27005 standards depict many similarities. However, NIST SP 800-30 lends itself to developing statements about future risks to be able to design mitigation plans, while ISO 27005 enables the variability of the procedures to be able to react promptly to new challenges (Salnyk et al., 2020). Wangen et al. (2018) highlights that a special feature of FAIR is also to carry out focused quantitative assessments and therefore differs from NIST SP 800-30 and ISO 27005. ISO 27005 refers to the CIA triad i.e., Confidentiality, Integrity and Availability and enables compliance with the regulations of the GDPR (Schäffter, 2015). However, this framework also presents

challenges especially for SMEs that have limited financial and human resources. Therefore, quantitative methods within the framework of ISO 27005 can overwhelm small companies.

The Monte Carlo simulation of the Open FAIR Model offers a comparatively simple way to carry out a quantitative analysis (Genest & Gamache, 2020). Open FAIR is designed to work with and be compatible with several other alternative standards including ISO 27005, which can be used to demonstrate to clients that industry standards and policies are being followed and therefore, create a good symbiosis with the Open FAIR model.

Since ISO 27005 is an international standard, while NIST SP 800-30 is a US standard, the following frameworks were selected to proceed with the risk analysis:

- Open FAIR (Monte Carlo Simulation)
- ISO 27005

The ISO/IEC 27005 standard consists of six phases depicted by Figure 1 below:

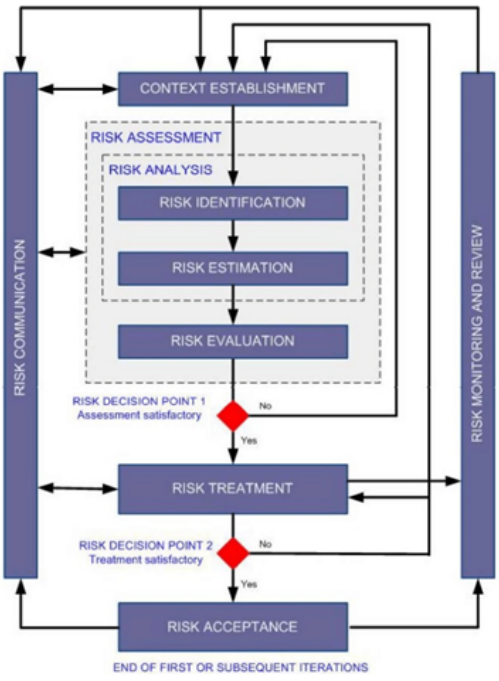


Figure 1: The ISO 27005 Risk Management workflow by Ionita et al. (2014)

The defined essential steps for the management of information security by the ISO 27005 standard are described in the Table 5 (Appendix A).

Risk Analysis

Marcelino-Sádaba et al. (2013) argue that risk assessments for SMEs should lean more toward qualitative methods, whereas Hubbard (2019) argues vehemently that quantitative methods should be used in every case. As such, a decision has been made to include both.

Solution Analysis

A comprehensive risk analysis was performed as shown in Table 6 (Appendix B) by utilising the above-mentioned frameworks as well as a risk assessment matrix (shown in Figure 2 below). Due to the company's low appetite for risk, as detailed in the status report, a risk appetite value of 4 has been assigned for the analysis.

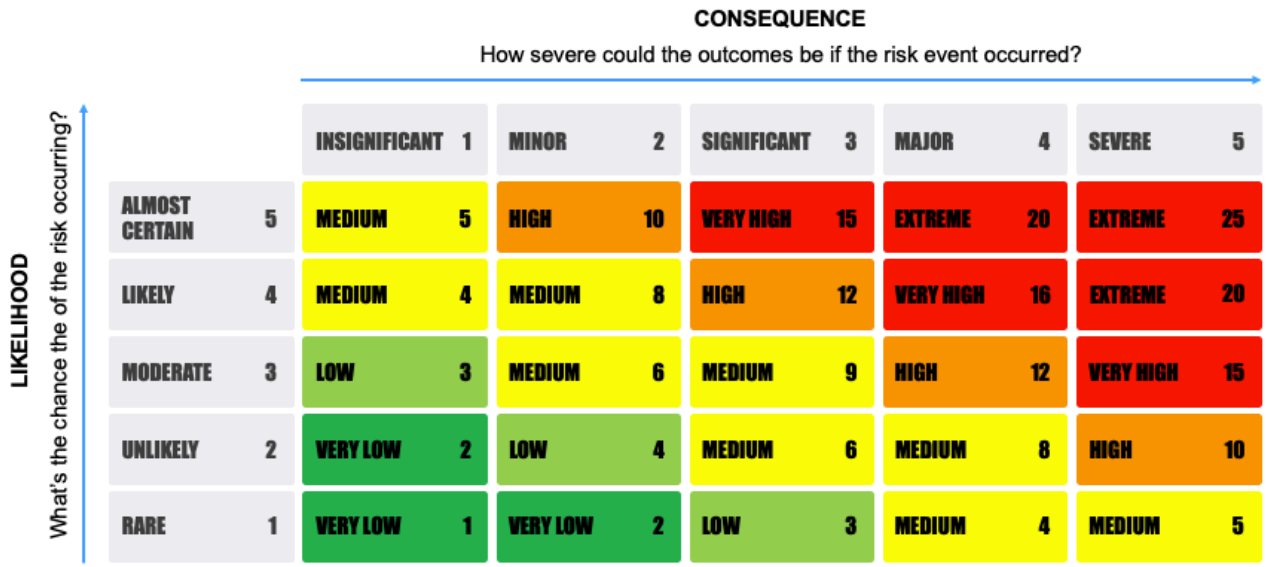


Figure 2: ***Risk Assessment Matrix (HiSide.io, N.D.)***

The results from Table 6 (Appendix B) can be summarised by Figure 3 below for all ERP solution options.

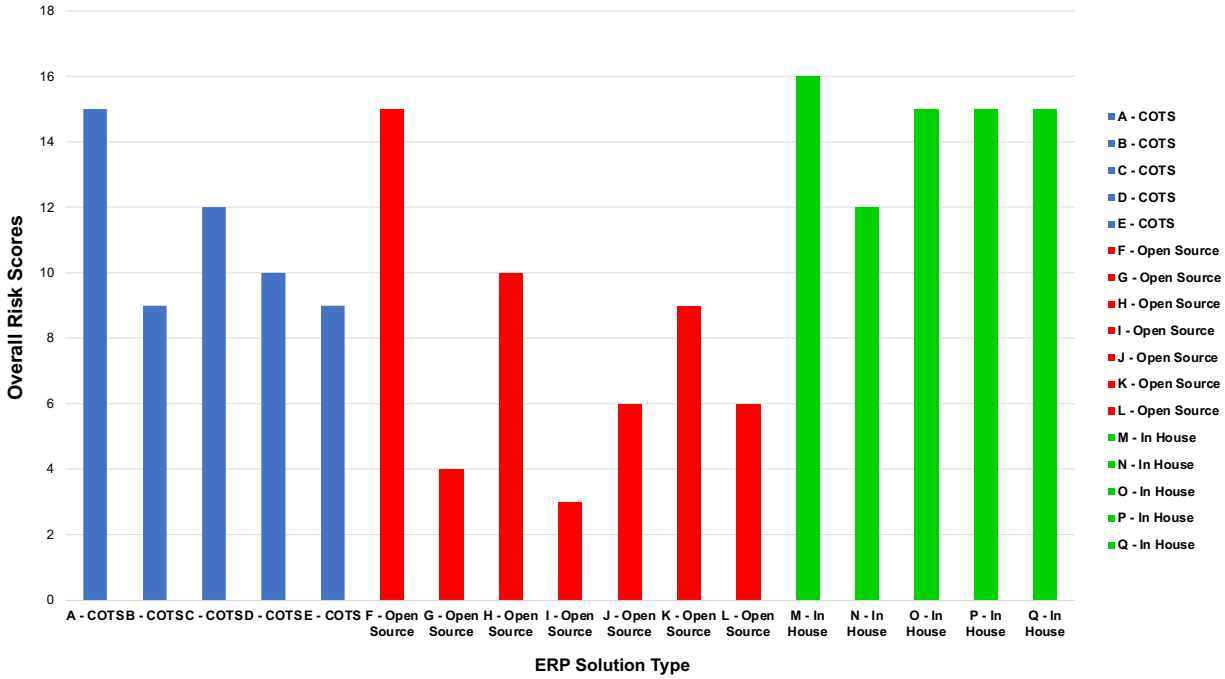


Figure 3: Risk Assessment Scores

As indicated in Figure 3 above, the open source solution produced slightly lower risk scores than the COTS and In-House solutions. In addition, to demonstrate a quantitative approach an Open Fair simulation was performed. The results are indicated in Appendix C.

Cost Benefit Analysis

In addition to the risk assessment analysis performed in Table 6 (Appendix B), Figure 4 below represents the cumulative risk scores for each ERP solution type.

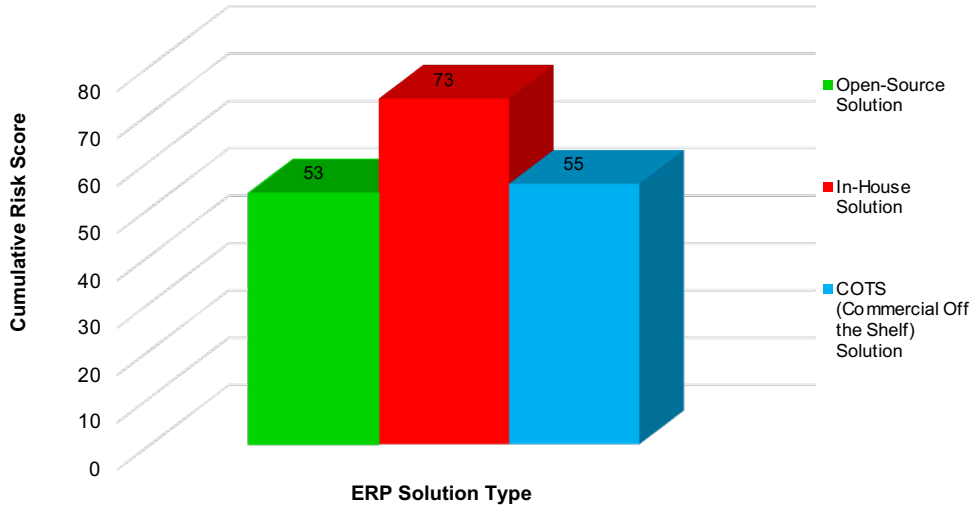


Figure 4: Cumulative Risk Scores for ERP Solutions

The In-House solution produced the highest cumulative risk score with the Open-Source solution being the lowest. This can be attributed to the following risks (In-House solution):

- Student lack of experience in programming may lead to incorrect architecture and/or design flaws (Roy et al., 2015).
- Risk of developer resigning and insufficient knowledge transfer to existing staff (code changes not possible).

According to Haddara (2011), there are various cost factors that affect ERP implementations in SME's, Figure 5 below represents these cost factors highlighting estimate percentages for each factor:

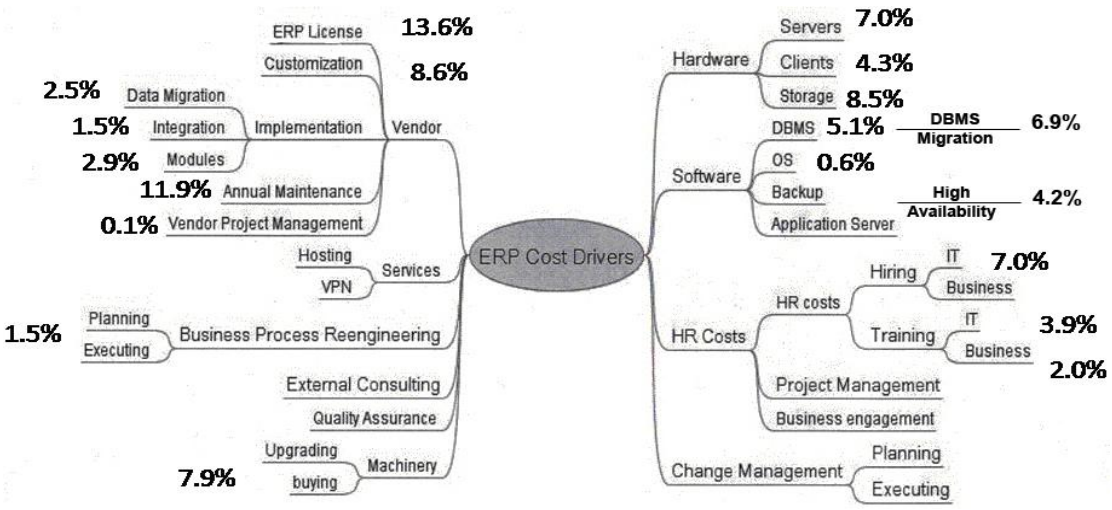


Figure 5: ERP Cost Drivers (Haddara, 2011)

By utilising the above figure as a guideline Table 1 below was created for each ERP solution:

Table 1: Cost Estimation

Costs Factors (per annum)	Description	Percentage of Total Cost (Haddara, 2011)	Solution		
			COTS (Commercial Off the Shelf) Solution	Open-Source Solution	In-House Solution
Once Off Purchase	Inlcudes once-off purchase price from vendor including software license (not appplicable to Open-Source & In-House Solution)	13,60%	$100 000,00	-	-
Infrastructure	Includes all hardware, networking & storage costs	19,80%	$145 588,24	$145 588,24	$145 588,24
Software	Includes Operating System costs (Windows / Linux) & Client Workstation Software. This is estimated to be around 4% for the Open-Source & In-House solutions as no vendor sofware is required on client machines.	6,00%	$44 117,65	$29 411,76	$29 411,76
Human Resources	Includes hiring of additional staff, project management & business engagement to support solution. Additional Developer required for In-House solution (further 10% of total cost)	30,90%	$227 205,88	$227 205,88	$294 117,65
Training	Includes training all staff to work on the new system	5,90%	$43 382,35	$43 382,35	$43 382,35
Support & Maintenance	Support & Maintenance costs provided for COTS solution i.e. $50k	6,80%	$50 000,00	-	-
Business Process Reengineering	Changing of business processes to accommodate ERP system	1,50%	$11 029,41	$11 029,41	$11 029,41
Add-Ons / Customisation	Customisation required to meet business requirements	8,60%	$63 235,29	$63 235,29	-
DBMS Migration	Database Migration	6,90%	$50 735,29	$50 735,29	$50 735,29
TOTAL		**100%**	**$684 558,82**	**$570 588,24**	**$523 529,41**

The method used to determine the overall cost for each solution can be found in Appendix D. Based on the above analysis, the COTS solution proved to be the most expensive ($684 558) while the In-House solution proved to be the cheapest ($523 529). However, the cumulative risk (blue bar in Figure 4) associated with the In-House solution does not align with the risk appetite of ACME Manufacturing. Therefore, the IT risk consultants recommend the Open-Source solution ($570 588) as being the most cost effective. It should also be noted the above cost-benefit exercise is a theoretical one and is based on assumptions and market related figures (Carlton et al., 2020).

Disaster Recovery Solution

According to VMware Inc. (2022), Disaster Recovery (DR) can be defined as "an organisation's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber-attack, or even business disruptions related to the COVID-19 pandemic**".** ACME Manufacturing requires a Disaster Recovery Plan (DRP) which provides guidance and information on how to respond to disasters, this plan can be found in Appendix E.

RPO and RTO Calculation

ACME Manufacturing has asked for a Recovery Point Objective of 15 minutes and a Recovery Time Objective of 4 hours. A profit loss calculation (detailed in Appendix E) was performed based on RTO values of 1 and 4 hours as depicted in Table 2 below:

Table 2: Profit Loss Calculation

Item	Unit	No Downtime	RTO of 4 hours	RTO of 1 hour
Workday (hours 8am - 6pm)	Hours	10	6	9
Profit per day	$	$1 366,67	$820,00	$1 230,00
Percentage Profit Loss	%	0%	40%	10%

From Table 2 above it is evident that the 'No Downtime' option is preferred since the company would not experience any profit loss. However, 'No Downtime' (Hot standby) solutions are expensive (AWS, 2022) and would significantly impact the company's bottom line. Furthermore, An RTO of 4 hours and a 40% profit loss per day would not align with ACME Manufacturing's appetite for risk. It is therefore recommended that the RTO for ACME Manufacturing be adjusted to 1 hour. This will ensure that ACME Manufacturing appetite for risk is satisfied, and the company operates and remains profitable.

Cloud Solution

It is recommended that ACME manufacturing adopts a cloud-based DR solution. Prakash et al. (2012) argue that to ease the burden on the IT department as well as reduce the cost of IT infrastructure a DR solution should be hosted in the cloud. Furthermore, Andrade et al. (2017) mention that many SME's have been adopting the Disaster-Recovery-as-a-Service (DRaaS) cloud-base solutions to guarantee availability as well save costs. Table 3 below provides a comparison of a traditional DR vs. a DRaaS (Rebah & Sta, 2016):

Table 3: Traditional DR vs. DRaaS

	Traditional DR	**DRaaS**
DR Site	Hosted on Premises, requires the insallation of power, cooling, backup servers as well as network connectivity.	Hosted and maintained in the cloud by a cloud provider
Human Resources	Requires additional resources to maintain data center i.e. server engineers, cabling technicians, network engineers, etc.	Resources are employed by cloud provider to maintain cloud infrastructure
Switching time to DR Site	Requires manual intervention and can happen within a few hours	Switching to DR can be automated and can happen within minutes
Cost	Investment in hardware and software required - expensive	Hardware and software provided at a subscription rate - cheaper
Regulatory Compliance	Requires in-house compliance experts to ensure GDPR compliance	GDPR compliant

By analysing the results in the above table, it is clear that ACME Manufacturing should proceed with a DRaaS solution. There are other factors to consider when comparing a traditional DR to a DRaaS, however the ones provided in the table above are sufficient to make an informed decision.

Disaster Recovery Solution Diagrams

Figure 6 below represents a block diagram of a DR solution extracted from Andrade et al. (2017). This figure would be applicable to the ACME Manufacturing environment. The components are detailed in Appendix F.

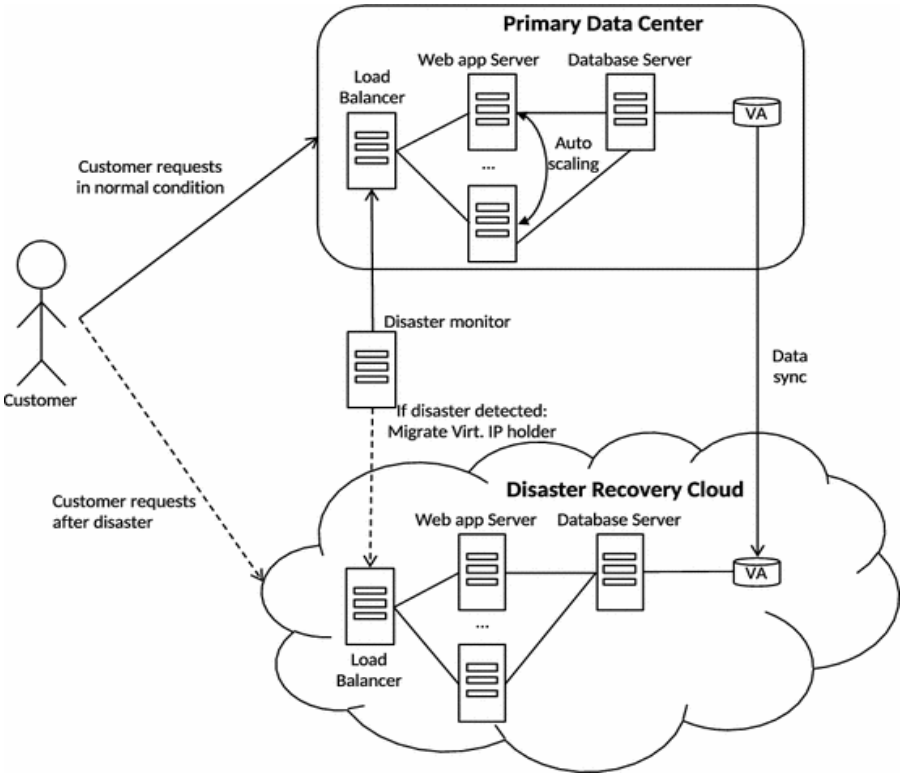


Figure 6: DR Solution for ACME Manufacturing (Andrade et al., 2017)

Based on ACME Manufacturing's RPO and RTO values, there are two possible DR strategies for a cloud-based ERP system viz.

- Warm Standby – a scaled down version of the production environment with minimal servers running. Database replication is present.
- Pilot Light – similar to the warm standby solution however no servers are running (switched off). Database replication is present.

The IT risk consultants recommend proceeding with a Pilot Light DR solution satisfying the requirements of resiliency, redundancy and network security. All servers (with the exception of the DB) will remain switched off in the DR site eliminating additional costs. Furthermore,

together with asynchronous replication of the databases between the two sites, the RPO of 15 minutes would be satisfied. A DR action plan is listed in Appendix F.

The IT Risk consultants are familiar and have experience hosting a pilot light DR solution in the Amazon Web Services (AWS) cloud. Figure 7 below provides a detailed representation of the solution (AWS, 2022), further explained in Appendix F.

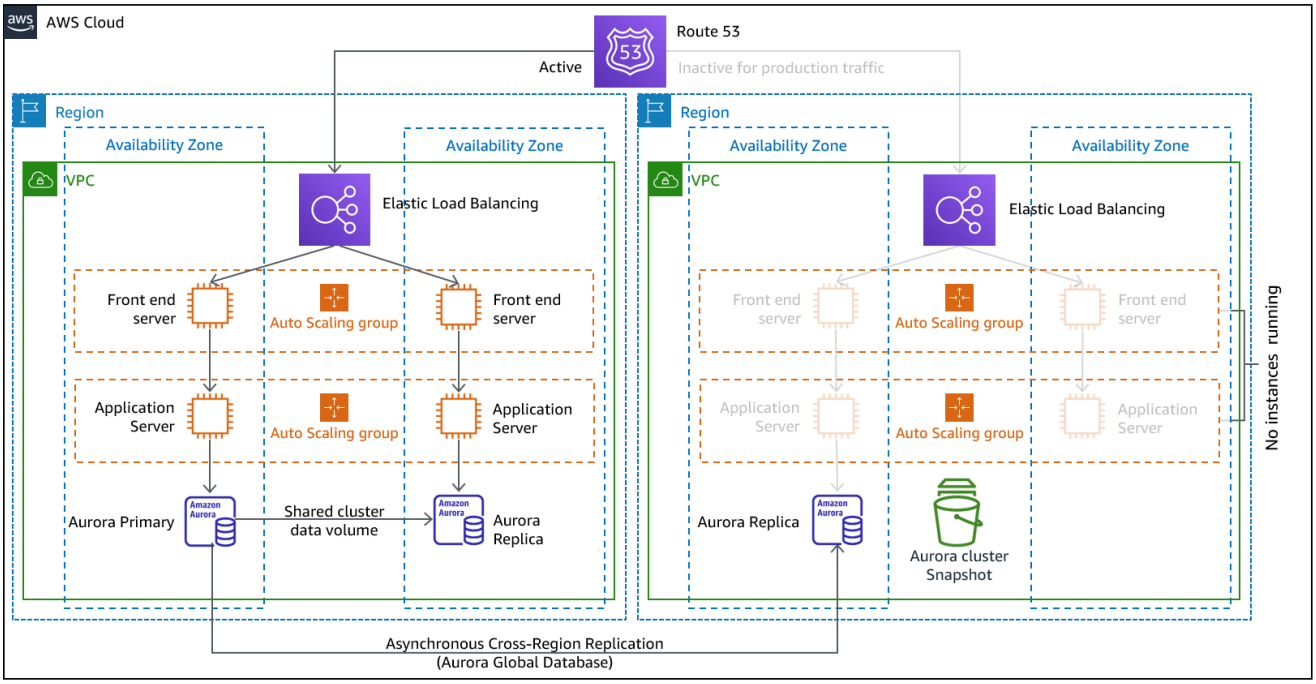


Figure 7: Pilot Light DR Solution for ACME Manufacturing in the AWS cloud (AWS, 2022)

Backups

If there is a complete site failure, local backups become inaccessible placing the business at risk. It is for this reason off-site backups become a requirement and forms part of a DR solution. Backups must be automatically generated every 10 minutes (between 8 am and 6 pm) and stored in a remote location. Furthermore, there should be an automatic daily backup between 6pm and 8am, thereafter the 10-minute daily backup for the previous day can be discarded.

Recommendations

The IT risk consultants recommend the following:

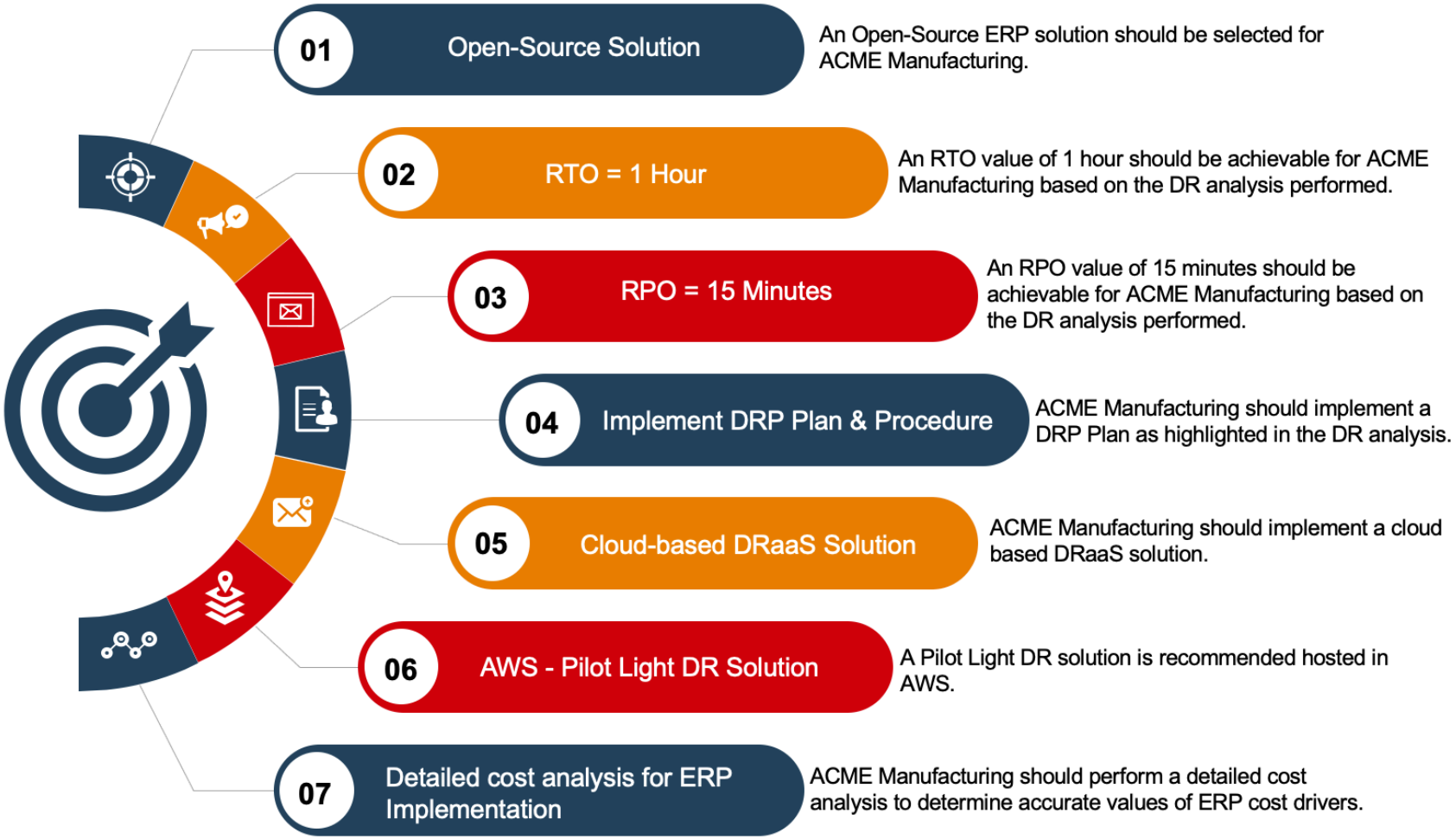


Figure 8: Final Recommendations

References

Amini, A. & Jamil, N. (2018) A Comprehensive Review of Existing Risk Assessment Models in Cloud Computing. *Journal of Physics: Conference Series.* 1018(1): 2-9. Available from: https://iopscience.iop.org/article/10.1088/1742-6596/1018/1/012004/meta [Accessed 10 April 2022].

Andrade, E., Nogueira, B., Matos, R., Callou, G. & Maciel, P. (2017) Availability modeling and analysis of a disaster-recovery-as-a-service solution. *Computing* 99(1): 929–954. Available from: https://link.springer.com/content/pdf/10.1007/s00607-017-0539-8.pdf [Accessed 10 April 2022].

AWS (2022) Amazon Web Services - Business Continuity Plan (BCP). Available from: https://docs.aws.amazon.com/whitepapers/latest/disaster-recovery-workloads-on-aws/business-continuity-plan-bcp.html [Accessed 10 April 2022].

Carlton, R., Beeson, K. & Meade, M. (2020) ERP Software Pricing Guide. Available from: https://www.erpfocus.com/erp-cost-and-budget-guide.html [Accessed 14 April 2022].

Clark, D. (2022) Median profit made by small and medium enterprises (SME) in the United Kingdom (UK) in 2020, by enterprise size. Available from: https://www.statista.com/statistics/291299/average-profit-of-smes-in-the-uk-by-enterprise-size/ [Accessed 20 March 2022].

DBA Manufacturing (2022) Frequently Asked Questions. Available from: https://www.dbamanufacturing.com/faq/ [Accessed 14 April 2022].

Genest, M. C. & Gamache, S. (2020) Prerequisites for the Implementation of Industry 4.0 in Manufacturing SMEs. Procedia Manufacturing. 51: 1215-1220. Available from: https://www.sciencedirect.com/science/article/pii/S2351978920320278 [Accessed 11 April 2020].

Haddara, M. (2011) ERP Cost Factors in SMEs. European, Mediteranean & Middle Eastern Conference on Information Systems. Available from: https://www.researchgate.net/profile/Moutaz-Haddara/publication/220023124_ERP_Cost_Factors_in_SMEs/links/00b49523dc6ea9b418000000/ERP-Cost-Factors-in-SMEs.pdf?origin=publication_detail [Accessed 12 April 2022].

HiSlide.io (N.D.) Risk assessment 5x5 matrix template. Available from: https://hislide.io/product/risk-assessment-5x5-matrix-template/ [Accessed 15 April 2022].

Hubbard, D. W. (2019) The Failure of Risk Management: Why It's Broken and How to Fix It. Hoboken: John Wiley & Sons. Available from: https://search.ebscohost.com/login.aspx?direct=true&db=nlebk&AN=2381255&site=ehost-live [Accessed: 12 April 2022].

IBM Cloud Education (2020) Monte Carlo Simulation. Available from: https://www.ibm.com/uk-en/cloud/learn/monte-carlo-simulation [Accessed 12 April 2022].

Ionita, D., Hartel, P., Pieters, W. & Wieringa, R. (2014) Current Estabilshed Risk Assessment Methodologies and Tools. Available from: https://www.researchgate.net/publication/308887387_Current_Established_Risk_Assessment_Methodologies_and_Tools [Accessed 10 April 2022].

ISO (2022) ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements. Available from: https://www.iso.org/obp/ui/#iso:std:iso:22301:ed-2:v1:en [Accessed 10 April 2022].

Le-Brun, P. (2022) Misunderstandings about vendor lock-in. Available from: https://aws.amazon.com/campaigns/uk-enterprise-executive-leaders/vendor-lock-in-blog/ [Accessed 12 April 2022].

Marcelino-Sádaba, S., Pérez-Ezcurdia, A., EcheverríaLazcano, A. M., & Villanueva, P. (2013) Project risk management methodology for small firms. Available from: https://www.sciencedirect.com/science/article/pii/S0263786313000665 [Accessed 12 April 2022].

Prakash, S., Mody, S., Wahab, A., Swaminathan, S., & Paramount, R. (2012) 'Disaster recovery services in the cloud for SMEs', *International Conference on Cloud Computing Technologies, Applications and Management (ICCCTAM).* Dubai, 8-10 December 2012. USA: IEEE. Available from: https://ieeexplore.ieee.org/document/6488087. [Accessed 17 April 2022].

Rebah, H. B., & Sta, H. B. (2016) *Disaster Recovery as a Service: A Disaster Recovery Plan in the Cloud for SMEs. 2016 Global Summit on Computer & Information Technology (GSCIT).* Tunisia, 16-18 July 2016. USA: IEEE. Available from: https://ieeexplore.ieee.org/abstract/document/7976645 [Accessed 10 April 2022].

Rittenburg, L. & Martens, F. (2012) Understanding and Communicating Risk Appetite. Committee of Sponsoring Organizations of the Treadway Commission. Available from: https://www.coso.org/Documents/ERM-Understanding-and-Communicating-Risk-Appetite.pdf [Accessed 20 March 2022].

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. Available from: https://doi.org/10.1007/978-81-322-2653-6_9 [Accessed 23 March 2022].

Salnyk, S., Sydorkin, P., Nesterenko, S., Zaytcev, A. & Konotopetc, M. (2020) Comparative analysis of the us ISO and NIST standards on assessing the risk of information leakage in communication systems. Journal of Scientific Papers "Social Development and Security. 10(6):1-11. Available from: https://paperssds.eu/index.php/JSPSDS/article/view/251/276 [Accessed 10 April 2022].

Schäffter, M. (2015) The EU Generals Data Protection Regulation: A Game Changer in Data Protection Management? Available from: https://www.researchgate.net/profile/Markus-Schaeffter/project/GDPR-Compliant-Data-Protection-Management-System/attachment/5b7fc0c6cfe4a76455ede710/AS:663067746652160@1535099078224/download/20151026+RiskorientedDPM.pdf?context=ProjectUpdatesLog [Accessed 10 April 2022].

The Open Group. (2018) Open FAIR™ Tool with SIPmath™ Distributions: Guide to the Theory of Operation. Available from: https://publications.opengroup.org/downloadable/download/link/id/MC40NDA4NjUwMCAxNjQ4OTA0MzE2MTM4MzcyMDE0MTUzODg4Njc%2C [Accessed 14 April 2022].

Ulven, J. & Wangen, G. (2021) A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet. 13(2): 39. Available from: https://www.mdpi.com/1999-5903/13/2/39 [Accessed 10 April 2022].

VMware Inc. (2022) What is Disaster Recovery? Available from: https://www.vmware.com/topics/glossary/content/disaster-recovery.html [Accessed 14 April 2022].

Wangen, G., Hallstensen, C. & Snekkenes, E. (2018) A framework for estimating information security risk assessment method completneness. International Journal of Information Security. 17(6): 681-699. Available from: https://link.springer.com/article/10.1007/s10207-017-0382-0 [Accessed 05 April 2022].

Appendices

Appendix A – Risk Assessment Frameworks

Table 4: Methodology comparison based on Wangen et al. (2018)

Risk identification method:	NIST 800-30	ISO-27005	FAIR	OCTAVE
Risk Identification				
Preliminary assessment	XX	-	X	XX
Risk criteria determination	-	XX	X	XX
Cloud-specific consideration	X	-	XX	-
Business objective identification	-	XX	XX	XX
Key risk indicators	-	-	XX	-
Stakeholder identification	-	XX	XX	X
Stakeholder analysis	-	-	XX	-
Asset identification	-	XX	XX	XX
Mapping of personal data	X	X	X	X
Asset evaluation	X	X	XX	X
Asset owner and customer	-	XX	X	XX
Asset container	-	-	-	XX
Business process identification	X	XX	-	-
Vulnerability identification	XX	XX	X	X
Vulnerability assessment	XX	XX	-	-
Threat identification	XX	XX	XX	XX
Threat assessment	XX	XX	-	XX
Control identification	XX	XX	-	X
Control assessment	-	XX	-	-
Outcome identification	XX	XX	X	XX
Outcome assessment	-	XX	-	X
Risk Estimation				
Asset identification and evaluation	X	-	-	-
Threat willingness/motivation	XX	XX	-	XX
Threat capability (know how)	XX	X	XX	
Threat capacity (Resources)	-	X	XX	X
Threat attack duration	-	-	XX	-
Vulnerability assessment	XX	-	XX	-
Control efficiency assessment	X	X	XX	-
Subjective probability estimation for event	XX	XX	XX	X
Quantitative probability estimation for event	XX	XX	XX	-
Subjective impact estimation	XX	XX	XX	XX
Quantitative impact estimation	-	XX	XX	X
Privacy risk estimation	X	-	-	-
Utility and incentive calculation	-	-	-	-
Cloud vendor assessment	X	-	X	-
Opportunity cost	-	X	-	-
Level of risk determination	-	XX	-	-
Risk aggregation	XX	XX	-	X
Risk Evaluation				
Risk criteria assessment/revision	-	X	-	X
Risk prioritization/evaluation	XX	XX	XX	XX
Risk treatment recommendation	-	-	-	XX
Completeness/Evaluation				
Phase				
1. Risk identification	18	30	22	24
2. Risk estimation	18	18	19	8
3. Risk evaluation	2	3	2	5
Completeness sum	38	51	43	37
Score:	Definition:			
XX	Addressed			
X	Partially addressed			
-	Not addressed			

Table 5: ISO 27005 Risk Management phases (Ionita et al., 2014)

ISO 27005 Risk Management phase	Description
Context establishment	The definition of the framework conditions then includes the establishment of criteria for the assessment and acceptance of risks, the delimitation of the area under consideration and the establishment of an organisation for risk management.
Risk identification	Risks are identified by recording all corporate values that are in the area under consideration. It is important to ensure that corporate values not only include hardware and software, but also business processes and information. The next step is to determine the consequences that can arise when a threat encounters a vulnerability. Consequences include loss of business volume or reputation.
Risk estimation	The risk can be assessed based on various influencing factors such as the criticality of company values, the extent of vulnerabilities or the effects of known security incidents. To assess risks, the consequences must firstly be assessed, more precisely the extent of damage in the event of a breach of confidentiality, integrity, or availability. On the other hand, the probability of such a security incident occurring must be determined. Finally, a risk level is determined by combining the extent of damage and the probability of occurrence.
Risk evaluation	This step is provided in the standard for prioritising the risks. The prioritisation can be done, for example, by prioritising risks for company assets that support less important business processes.
Risk treatment	A decision must be made as to whether a risk should be reduced, accepted, avoided, or transferred. While appropriate security measures must be defined to mitigate, risks that meet the residual risk acceptance criteria can be left unaddressed. A risk can be avoided, for example, by placing a critical system in a protected environment where it is better protected against natural disasters. Risks can be transferred to third parties through insurance or through appropriate contract formulations.
Risk acceptance	The result of the risk treatment is a plan that shows the corresponding recommendations for action for each risk. The top management of an organisation can decide to accept risks even if they do not meet the acceptance criteria. In these cases, a formal assumption of risk is required.

Appendix B – Solution Analysis

Table 6: Solution Analysis

Type of Risks	Solution	Graph Reference	Risk Appetite = 4							
			Risks	Approach (Qualitative / Quantitative)	Rationale / Justification (Using the Risk Assessment Matrix)	Weightings (Using the Risk Assessment Matrix)	Overall Risk Scores	Cumulative Risk Scores	Recommendations - Risk Treatment (Avoided, Retained, Shared, Reduce or Transferred)	Mitigations
Solution Specific Risks	COTS	A - COTS	The company liquidates or is acquired and the product becomes EOL (End of Life).	Qualitative	Liquidation of companies are always a possibility, this risk would be classified as a severe consequence (5) and a moderate likelihood (3).	Likelihood - Moderate - 3 Consequence - Severe - 5	15	55	Reduce / Transfer	ACME Manufacturing should sign a contract with the vendor for extended support should the product become EOL, this should be for at least 24 months after the EOL date has occurred. This contract would provide ACME manufacturing suffiicient time to perform a risk assessment and cost analysis to determine a way forward. A software escrow could also be initiated.
		B - COTS	ERP solution is generic and does not align or fit with existing business processes (Buonanno et al., 2005). The system is not able to integrate with existing systems and / or does not cater for all the companies requirements (Ojala et al., 2006).	Qualitative	It is very common that ERP systems are desgined to fit most companys' generic process however the possiblity exists that not all requirements will be satisfied. This risk will be classified as a 'moderate' likelihood (3) with a 'significant' consequence (3).	Likelihood - Moderate - 3 Consequence - Significant - 3	9		Reduce	Comprehensively compare the software programs available to determine if the software matches ACME Manufacturing's requirements. Involve system owners in the requirements gathering at every opportunity.
		C - COTS	Purchasing an ERP system that is not easily customisable and are not flexible to business changes (too rigid).	Qualitative	This risk falls into the 'likely' category (4) for Likelihood (3) and the 'significant' category for consequence as vendors do offer capabilities to customise their systems at additional costs.	Likelihood - Likely - 4 Consequence - Significant - 3	12		Avoid	Comprehensively compare the software programs available to determine if the software matches ACME Manufacturing's requirements.
		D - COTS	Vendor lock-in, risk of rising support costs as product matures (Opara-Martins et al., 2016).	Qualitative	This risk will be classified as 'almost certain' (5) Likelihood since support costs increases anually for every product purchased. ACME Manufacturing would need to absorb the rise in support cost classifying the consequence as 'minor' (2).	Likelihood - Almost Certain - 5 Consequence - Minor - 2	10		Reduce	ACME Manufacturing could negotiate contract terms to have support costs fixed for a period e.g. 5 years. Include SLAs to ensure software vendor performs as expected.
		E - COTS	Features and functionalities are dependent on the company's roadmap.	Qualitative	COTS software which exactly fits the company's roadmap. The consequences could be significant, although some working software is still possible.	Likelihood - Moderate - 3 Consequence - Significant - 3	9		Avoid / Reduce	Comprehensively compare the software programs available to determine if the software matches ACME Manufacturing's requirements. Disable any features that are not required.

Type of Risks	Solution	Graph Reference	Risk Appetite = 4							
			Risks	Approach (Qualitative / Quantitative)	Rationale / Justification (Using the Risk Assessment Matrix)	Weightings (Using the Risk Assessment Matrix)	Overall Risk Scores	Cumulative Risk Scores	Recommendations - Risk Treatment (Avoided, Retained, Shared, Reduce or Transferred)	Mitigations
Solution Specific Risks	Open-Source	F - Open Source	Possibility of not being from a trustworthy source.	Qualitative	Open-source software is freely available to the public for downloads. There is possibility that the source is untrusted. Downloads should only be made from a reputable site. In the event that untrusted software is downloaded, the company would experience a major security threat.	Likelihood - Moderate - 3 Consequence - Major - 5	15	53	Avoid	Use known and trusted source communitiy sources, and use md5checksum available to verify author / source
		G - Open Source	No dedicated enterprise support in the event that urgent support is needed.	Qualitative	Open-source software does not have dedicated support teams, instead the software relies on the developer and the community to be updated.	Likelihood - Likely - 4 Consequence - Insignificant - 1	4		Retain	Rely on community support
		H - Open Source	Data Security and confidentiality	Qualitative	Unlikely for personal data to be exposed to Open Source provider, however there may be security holes in the software even though it is community reviewed. Data breaches can result in heavy fines and a loss of reputation.	Likelihood - Unlikely - 2 Consequence - Severe - 5	10		Reduce	Ensure secure coding, end user awareness training, and Non Disclosure Agreements (NDA)
		I - Open Source	Software not clearly documented explaining features and functionality.	Qualitative	On the contrary to the risk identified, comprehensive documentation for open-source software exists and is contnually updated by the community.	Likelihood - Rare - 1 Consequence - Significant - 3	3		Retain	Documentation could be sought from developer, or created based on what ACME can glean from using it.
		J - Open Source	Acquiring an ERP system that is not easily customisable and are not flexible to business changes (too rigid).	Qualitative	With many systems available, it would only need an analysis to determine if the software was suitable, and open source software is customisable. However, if it did occur, it could be expensive and difficult to remedy once the software has been implemented.	Likelihood - Unlikely - 2 Consequence - Significant - 3	6		Avoid / Reduce	ACME Manufacturing should trial various options befpre choosing which software to use to understand if the code is easily customisable. Help can be sought from the online community, and finally expert staff can be employed if necessary.
		K - Open Source	ERP solution is generic and does not align or fit with existing business processes (Buonanno et al., 2005). The system is not able to integrate with existing systems and / or does not cater for all the company's requirements (Ojala et al., 2006).	Qualitative	It is very common that ERP systems are desgined to fit most companys' generic process however the possiblity exists that not all requirements will be satisfied. This risk will be classified as a 'moderate' likelihood (3) with a 'significant' consequence (3).	Likelihood - Moderate - 3 Consequence - Significant - 3	9		Reduce	Comprehensively compare the software programs available to determine if the software matches ACME Manufacturing's requirements. Involve system owners in the requirements gathering at every opportunity.
		L - Open Source	Difficult to refactor or modify source code (Roy et al., 2015).	Qualitative	With many systems available, it would only need an analysis to determine if the software was suitable. However, if it did occur, it could be expensive and difficult to remedy once the software has been implemented.	Likelihood - Unlikely - 2 Consequence - Significant - 3	6		Reduce / Avoid	Obtain help from the online community. Hire additional expert staff if required. Choose a software with modular code with smaller reusable components.

Type of Risks	Solution	Graph Reference	Risk Appetite = 4							
			Risks	Approach (Qualitative / Quantitative)	Rationale / Justification (Using the Risk Assessment Matrix)	Weightings (Using the Risk Assessment Matrix)	Overall Risk Scores	Cumulative Risk Scores	Recommendations - Risk Treatment (Avoided, Retained, Shared, Reduce or Transferred)	Mitigations
Solution Specific Risks	In-House	M - In House	ERP software is complex and often designed with business processes in mind. It is also linked closely with other external systems. The student may lack experience in these integrations and processes (Iskanius, 2009).	Qualitative	This is extremely likely that the student would have insufficient knowledge. A method would have to be introduced for the developer to check the code which is being written. This could cause functions and interfaces to be ineffective.	Likelihood - Likely - 4 Consequence - Significant - 4	16	73	Reduce	Ensure regular monitoring of progress, consultation and peer reviews between developer, stakeholder and manager. Document changes and backup of source code.
		N - In House	Risk of ERP software development being abandoned (student drops out of course).	Qualitative	Of course, this is always a possibility. The consequence would be large if knowledge was not shared, or documented properly.	Likelihood - Moderate - 3 Consequence - Major - 4	12		Reduce	Modularised and well-logged development of the ERP to be able to react to changes of the development team. Ensure good commenting of code, document any changes and backup source code.
		O - In House	Risk of developer resigning and insufficient knowledge transfer to existing staff (code changes not possible).	Qualitative	Of course, this is always a possibility. The consequence would be large, especially if it not documented properly, and the student may not have the support they need.	Likelihood - Moderate - 3 Consequence - Severe - 5	15		Reduce	Regular monitoring of progress, consultation and peer reviews between developer, stakeholder and manager. Ensure good commenting of code, document any changes and backup source code.
		P - In House	Student lack of experience in programming may lead to incorrect architecture and/or design flaws (Roy et al., 2015).	Qualitative	If the communication between the Developer and the student is poor then there is a chance of poorly designed code. If this should happen, there may be bigger problems later in the SDLC. Security holes may also be present	Likelihood - Moderate - 3 Consequence - Severe - 5	15		Reduce	Regular monitoring of progress, consultation and peer reviews between developer, stakeholder and manager. Provide guidance, document any changes and backup source code.
		Q - In House	Inexperienced test teams may lead to issues picked up late in the project, compromising completion times (Roy et al., 2015).	Qualitative	If issues are picked up late in the project, they may be more costly to fix later in the SDLC.	Likelihood - Almost Certain - 5 Consequence - Significant - 3	15		Reduce	Regular testing at each stage of the SDLC

Type of Risks	Solution	Graph Reference	Risk Appetite = 4							
			Risks	Approach (Qualitative / Quantitative)	Rationale / Justification (Using the Risk Assessment Matrix)	Weightings (Using the Risk Assessment Matrix)	Overall Risk Scores	Cumulative Risk Scores	Recommendations - Risk Treatment (Avoided, Retained, Shared, Reduce or Transferred)	Mitigations
Business Risks	All Solutions	ALL	Project overrunning	Qualitative	Very common in projects and is extremely likely, especially without a dedicated project manager. This should not cause any other consequence than additional staff time.	Likelihood - Almost Certain - 5 Consequence - Minor - 2	10	-	Reduce	Including buffer time for the project and regular review of the progress to adjust labor force if necessary.
		ALL	Change management challenges i.e., users are often hesitant to make use of new systems and may fallback to old procedures (Ojala et al., 2006).	Qualitative	Fairly likely as humans generally do not like change. However, this should not cause any consequence other than a need for involvement	Likelihood - Moderate - 3 Consequence - Minor - 2	6		Reduce	Include users at requirements gathering stage. Implement training workships to get them used to the new system, and maintain open communictation.
		ALL	Lack of human resources (including project managers and IT staff) involved in the ERP implementation project (Kettunen & Simons, 2001).	Qualitative	From the assumptions, there seems to be dedicated IT staff available to facilitate the ERP implementation. The consequence would be big if it were not managed and supported properly	Likelihood - Unlikely - 2 Consequence - Major - 4	8		Reduce	Ensure the assignement of a dedicated project manager, and IT department are assigned to support the implementation. Temporary staff may need to be hired, if necessary.
		ALL	Lack of technological resources to support ERP system.	Qualitative	The assumptions stated the IT Infrastructure was rudimentary. The project would likely need new systems installed. The ERP system would be slow, or fail if this risk were realised, halting progress of the business.	Likelihood - Likely - 4 Consequence - Major - 4	16		Reduce	According to ISO 31000:2018 Risk management guidelines, section 5.4.2 - Top management should be committed to make the necessary resources available (ISO, 2022). Infrastructure equipment is likely to be needed in the budget.
		ALL	Managers and end-users have different perspectives on ERP solutions (Amoako-Gyampah, 2004).	Qualitative	Possible if poor communication. However consequence only reuires more a higher lever of user involvement.	Likelihood - Unlikely - 2 Consequence - Minor - 2	4		Retain	Include user in the development and regular consultation of them in the individual phases of the SDLC.
		ALL	Lack of support and communication between company executives and IT department.	Qualitative	Management should be aware of the importance, due to the very nature of bringing the ERP system on board. Consequence could be large and lead to gathering the wrong requirements.	Likelihood - Unlikely - 2 Consequence - Severe - 5	10		Reduce	Include regular meetings so that IT can update the board on the progress of the budget. Ensure top management put their name to the work being done, and are present in any workshops.
		ALL	Inadequate system reliability and stability (Iskanius, 2009).	Qualitative	Has potential if not designed correctly. A failing system could cause halt in progress of the company, including full outages.	Likelihood - Likely - 3 Consequence - Severe - 5	15		Reduce	Introduce Change Control. Include High Availability Disaster Recovery measures
		ALL	Implementation of ERP system affects 'business as usual' tasks.	Qualitative	Possibile if not tested correctly. Could cause a halt in production.	Likelihood - Moderate - 3 Consequence - Severe - 5	15		Reduce	Parallel use of the new and old system in the implementation phase of the ERP. Use sandbox and pilot groups where possible.
		ALL	Inadequate or lack of documentation of ERP systems.	Qualitative	A system may not have sufficient documentation, especially if not a COTS solution. Would make it difficult to troubleshoot and realise its potential.	Likelihood - Likely - 4 Consequence - Minor - 2	8		Reduce	Ensure comprehensive library of policies, processes, standards and guidelines. Create user guides on how to run and maintain the software. If not possible, documentation shall be implemented as more knowledge is known of the system..
		ALL	Risk around disposal of secure data from the retired/old system (Roy et al., 2015).	Qualitative / Quantitative	Very possible as such data could be lying around for decades. Data breaches from careless disposal of data could lead to heavy fines and loss of trust from customers and third parties. Due to the high level of risk, this requires a further quantitative assessment.	Likelihood - Likely - 4 Consequence - Severe - 5	20		Reduce	Have data destroyed securely, by a specialist company that are able to produce a destruction certificate,
		ALL	Miscalculation of the planned financial plan / budget (Shahzad et al., 2010).	Qualitative	Possible if costs are not thoroughly analysed. Could lead to an unfinished product, or financial difficulty for the	Likelihood - Moderate - 3 Consequence - Major - 4	12		Reduce	Use statistical analysis, expert opinion and research of similar industry models.
		ALL	Incomplete recording of ERP requirements (Shahzad et al., 2010).	Qualitative	Could be very costly if the wrong product was purchased or designed.	Likelihood - Moderate - 3 Consequence - Severe - 5	15		Reduce	Extensive planning in the first phase of the SDLC. Consultation with system owners, top management, and key stakeholders.
		ALL	sufficient planning of future system requirements (Wallace et al., 2004)	Qualitative	Possible without a fully fledged analysis/forecasting. Could eventually result in obsolete product, in the future.	Likelihood - Moderate - 3 Consequence - Significant - 3	9		Reduce	Modularisation of the system, and forecast and analysis, where possible.

Appendix C - Monte Carlo Simulation

IBM define a Monte Carlo Simulation as “a mathematical technique, which is used to estimate the possible outcomes of an uncertain event” (IBM Cloud Education, 2020). They are useful to predict a series of hypothetical results for given inputs based on known figures and random variables.

For this analysis, the identified loss scenario is as follows:
“Anyone outside of the company could find a discarded disk drive and access it using skill and endeavour. Once accessed, they misuse sensitive information. When this event occurs, ACME Manufacturing always suffers primary productivity and response losses. Furthermore, the company could also suffer secondary response costs, fines and judgements.”

There has been no mention that ACME have any policies to enforce encryption of data on disk drives, for example. Therefore, it is assumed that if applied at all, it is only done on an ad-hoc basis. It is also assumed an SME of ACME’s stature uses usernames and passwords to access the company devices. It is assumed a number of disks containing sensitive data from the old system have been discarded, say 10.

Threat Event Frequency: The chance that someone will find the device is moderate, however the chance they will try to examine the data by advanced means is quite low. The threat event frequency is based on the threat capability and the resistance strength.

Threat Capability: The chances are that if a hard drive was found, it would not be investigated, and even if it were, most finders would not possess the skill and knowledge required to access secure data without the need for a username and password. The threat

capability does not change even after the solution and therefore, the threat capability rating is the same for both current and proposed solutions.

Resistance Strength: Due to the possibility of encryption, and the likelihood of usernames and passwords, the figures for Resistance Strength are given in Table 7 below:

Table 7: Open Fair Model Input Data

Metric	Minimum	Most Likely	Maximum
Threat Event Frequency per year (Current)	0.1	1	10
	(Once every 10 years)	(Once a year)	(10 times in a year)
Threat Event Frequency per year (Proposed):	0.1	0.2	5
	(Once every 10 years)	(Once every 5 years)	(5 times in a year)
Threat Capability per year (current and proposed)	5%	20%	95%
Resistance Strength (current)	30%	50%	90%
Resistance Strength (proposed)	90%	95%	99%

The quantitative risk assessment example has been carried out for one of the major risks found during the qualitative risk analysis viz. “Risk around disposal of secure data from the retired/old system”. The Open FAIR tool uses the Monte Carlo simulation method, and has been used to perform this risk assessment. This is built upon the proven statistical engine SIPmath (The Open Group, 2018). The analysis can be found in Appendix C and the results are indicated in Figure 9 below:

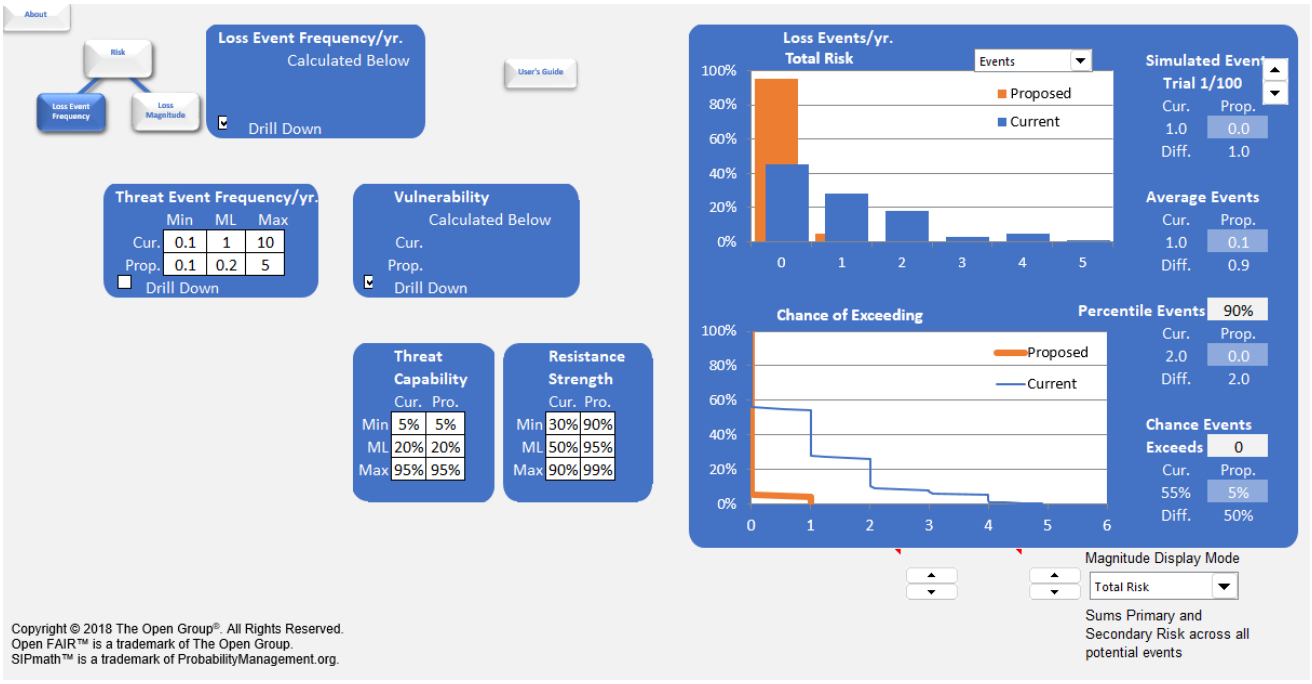


Figure 9: OpenFair Simulation

Securely disposing of old disks dramatically decreases the chance of a loss as seen in Figure 9 above (proposed solution in orange). The current results (blue) depict a 55% chance of a loss event in a year. When hiring a professional company to securely dispose of data, the proposed results (orange) show there is a 95% chance of 0 losses occurring in a year, and only 5% in 1 loss occurring which is a dramatic mitigation.

Appendix D – Cost Analysis

The following method was used to determine the overall cost for each solution:

- ‘Once off Purchase’ as well as ‘Support & Maintenance’ costs were provided by ACME Manufacturing as $100 000 (13.6% of the total cost) and $50 000 (6.8% of the total cost) respectively for the COTS solution.
- Infrastructure costs were estimated at 19.8%, similar infrastructure requirements would be applicable to all three solutions.
- Software costs were estimated to be 6% for the COTS solution and 4% for the Open-Source and In-House solution. The assumption is that vendor provided client applications will need to be installed in client machines (DBA, 2022) for the COTS solution, while the Open-Source and In-House solution will use the web browser to access the application.
- Human Resources (HR) cost is one of the higher estimates (30.9%) as this includes hiring additional staff, project management amongst others. A developer would be required for the In-House solution raising the HR costs as well.
- Training (5.9%), Business Process Reengineering (1.5%) and Database Management Systems (DBMS) Migration (6.9%) have similar costs for all three solutions.
- Lastly, Add-Ons / Customisation costs were estimated at 8.6% and would only be applicable to the COTS and Open-Source solution. The In-House solution will be built from scratch directly from the requirements specification and therefore no customisation is necessary.

Appendix E – DRP & RTO Calculations

Disaster Recovery Plan

The DRP is a subset of Business Continuity (BC) plans and should include the following items according to ISO (2022):

1. The purpose, scope and objectives of the plan.
2. The roles and responsibilities of the DR team that will implement the plan.
3. The action steps required to implement the DR plan.
4. Supporting information needed to activate operate, coordinate and communicate the team's actions.
5. Internal and external interdependencies.
6. The resource and reporting requirements.
7. A process for reverting back to the production system.

It is recommended that a DR team be implemented to ensure the above mention procedures are complied with.

RTO Calculations

ACME Manufacturing has asked for a Recovery Point Objective of 15 minutes and a Recovery Time Objective of 4 hours. These terms are defined as follows (AWS, 2022):

- RTO – the amount of downtime the business can tolerate (4 hours)
- RPO – the amount of data loss the business can endure (15 minutes)

Figure 10 below depicts a visual representation of RTO and RPO respectively (AWS, 2022)

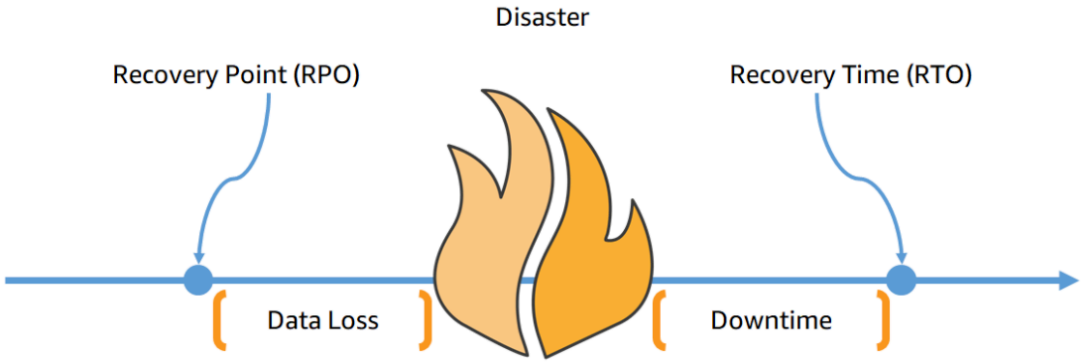


Figure 10: RPO and RTO Representation

In the status report, the following assumption was made and plays a vital role in the determination of RTO:

- The company has a low appetite for risk (Rittenburg & Mertens, 2012) and cannot afford or tolerate any interruption or downtime in its production line and subsequently affecting its revenue stream.
- The median profit of SME's (employee base between 50-249) operating in the UK is around $328,000 (Clark, 2022). It is assumed that ACME manufacturing's average profit is within this range.

The total profit per month is estimated to be $27,333 using the formulae below:

$$Profit\ per\ month = \frac{Annual\ Profit}{12} = \frac{\$328\,000}{12} = \$27{,}333$$

The company's operating hours is between 8am – 6pm equating to a 10-hour workday i.e., 200 hours per month (company does not operate on weekends i.e., 10 x 20 days = 200*h*).

The profit per hour and subsequent profit per day can be calculated as follows:

$$Profit\ per\ hour = \frac{\$\ 27{,}333}{200\ h} = \$136{,}67\ per\ hour$$

$$Profit\ per\ day = \ \$136{,}67\ per\ hour\ \times\ 10\ hours = \$\mathbf{1366.67}$$

Table 8 below summarises the above assumptions and calculations:

Table 8: Profit Calculation

Item	Unit	Value
Profit (per annum)	$	$328 000,00
Profit (per month)	$	$27 333,33
Workday (hours 8am - 6pm)	Hours	10
Working hours in a month	Hours	200
Profit per Hour	$	$136,67
Profit per Day	$	**$1 366,67**

If an **RTO of 4 hours** is selected i.e., the company only operates for 6 hours per day; the following profit loss calculation is applicable:

$$Profit\ per\ day_{(RTO=4)} = \$136{,}67\ per\ hour \times 6\ hours = \$820{,}00$$

$$\%\ Profit\ Loss = \left(\frac{Profit\ per\ day - Profit\ per\ day_{(RTO=4)}}{Profit\ per\ day}\right) \times 100 = \mathbf{40}\%$$

If an **RTO of 1 hour** is selected and the company operates for 9 hours per day; the following profit loss calculation is applicable:

$$Profit\ per\ day_{(RTO=1)} = \$136{,}67\ per\ hour \times 9\ hours = \$1230{,}00$$

$$\%\ Profit\ Loss = \left(\frac{Profit\ per\ day - Profit\ per\ day_{(RTO=1)}}{Profit\ per\ day}\right) \times 100 = \mathbf{10}\%$$

Table 9 below summarises the above calculations:

Table 9: Profit Loss Calculation

Item	Unit	No Downtime	RTO of 4 hours	RTO of 1 hour
Workday (hours 8am - 6pm)	Hours	10	6	9
Profit per day	$	$1 366,67	$820,00	$1 230,00
Percentage Profit Loss	%	0%	40%	10%

Appendix F – DR Solution

DR Action Plan

In the event of a disaster the following processes needs to be actioned (Rebah & Sta, 2016):

1. Power on all servers and confirm availability.
2. Ensure servers are connected to database and data integrity is verified.
3. Execute test cases and monitor for failures.
4. Switch traffic to DR site via DNS (Domain Name Service) or virtual IP addresses.

The above process can be executed in less than 1 hour manually, satisfying the RTO requirement.

DR Solution Diagram

Figure 11 below represents a block diagram of a DR solution extracted from Andrade et al. (2017). This figure would be applicable to the ACME Manufacturing environment.

. Components include a:

- Load Balancer (LB) – used to load balance traffic between regions
- Disaster monitor – used to monitor if a failure has occurred and trigger DR site
- Web Application Server – a server hosting the ERP application
- Database Server – used to house the ERP data.

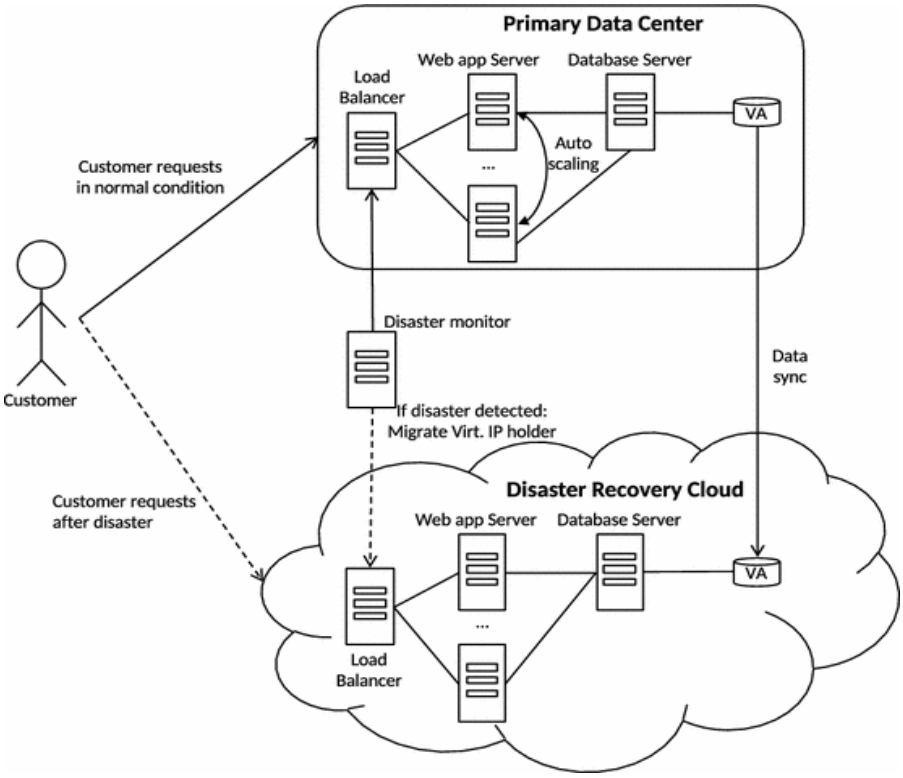


Figure 11: DR Solution for ACME Manufacturing (Andrade et al., 2017)

Pilot Light DR Solution

In Figure 12 below, *Route53* provides the DNS service to control the routing of traffic. Servers are places in a primary region (right) and replicated in a secondary region via the AWS backbone network. Regions can represent countries. Availability Zones represent data centers within a country. The *Elastic Load Balancer* provides the ability of distributing traffic between data centers. *Auto Scaling groups* provide the feature of scaling up/down as traffic increases/decreases. Databases (Aurora) are asynchronously replicated across regions. All servers are within a Virtual Private Cloud (VPC) providing an isolated and secure environment. By utilising services such as *Route53*, *Elastic Load Balancers*, *Auto Scaling groups* and asynchronous replication of the DB between regions; the overall solution is secure, resilient, highly available and fault tolerant. Furthermore, the AWS model is subscription based and easily migratable to another cloud provider, preventing vendor lock-in clauses (Le-Brun, 2022).

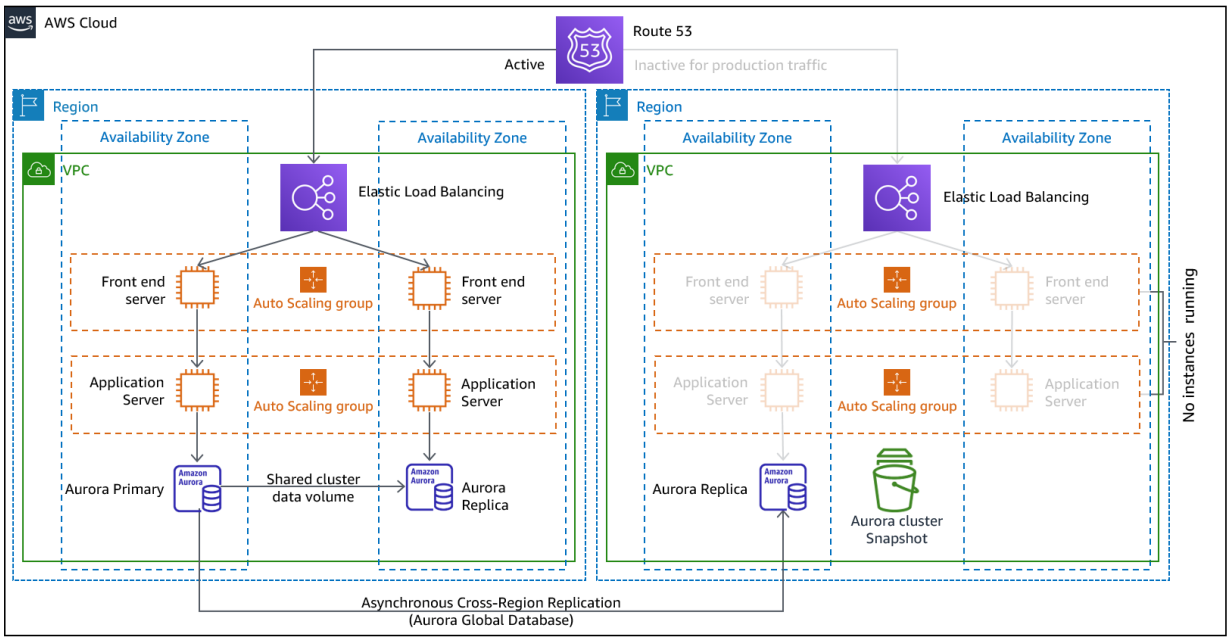


Figure 12: Pilot Light DR Solution for ACME Manufacturing in the AWS cloud (AWS, 2022)