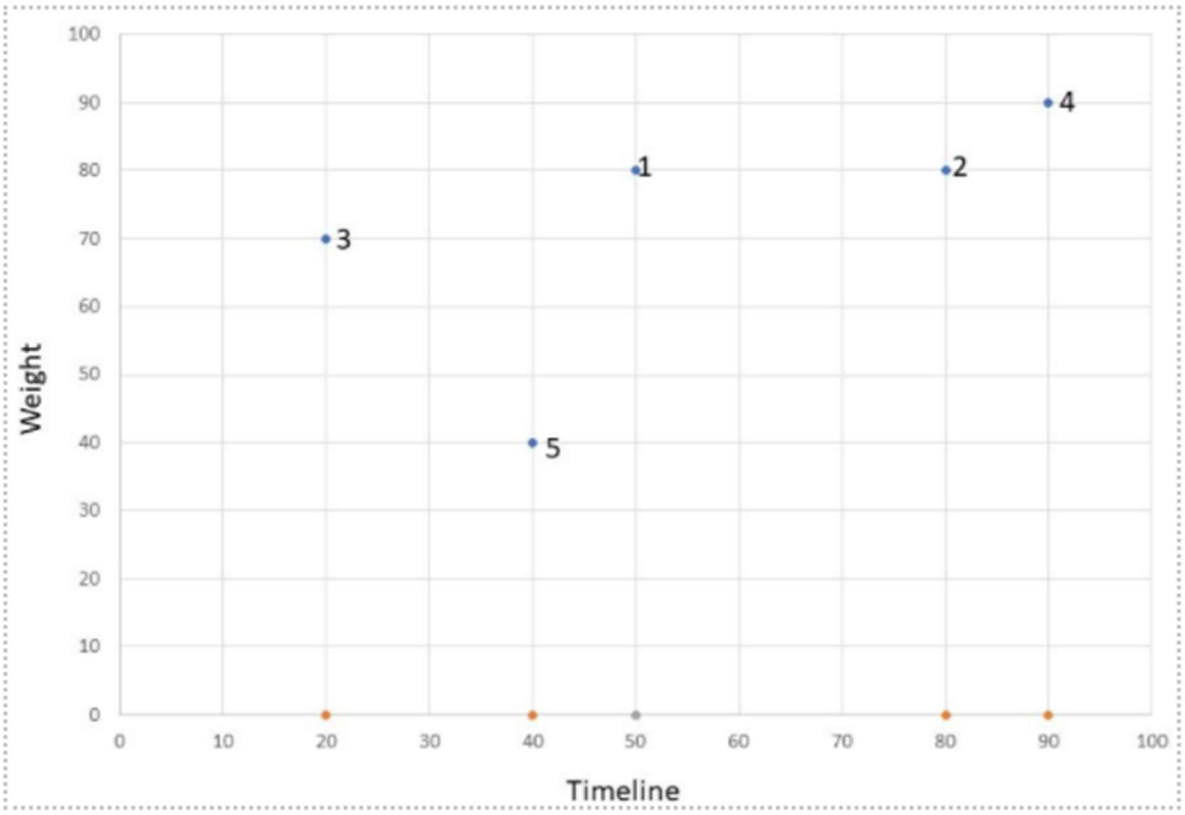
Development Team Project: Risk Assessment Report

Risk Assessment

A risk assessment is a process to identify potential hazards and analyse what could happen if a hazard occurs (Ready.gov, N.D). Below are the risks predicted risks



In this chart, the following numbers are assigned to different risks:

1. technology innovation: Rating - High

The new software to be implemented in Acme implies new technologies. When a project is set up, the implementation of new technology is fundamental because otherwise, it can cause a non-success in a project. Thus the risk of staff failing to use technology is high

2.application functionality: Rating - Medium

The users' needs in terms of functionality are very high, and they have to fulfil all the needs in terms of demand and response to their requirements. The system is off the shelf, and we expect functionality to be up to standard. Thus the risk is medium

3. Software architecture: Low

The architecture has an equally important weight when evaluating the risks. If a bad decision has been taken when setting up the architecture of a product, the risks can be considerable in terms of the performance and security of the application. This risk is low since a big experienced supplier has manufactured the system

4.Production/development: High

The production and development of the product is a significantly important part, as it has to respect what the users expect from the product as well as the demand from the management. This risk is high because the users were not involved during the

development stage, and as such, a complicated system may be purchased for a high cost that does not meet user needs

5. IT Management and Installation: Rating -Low

Project management can negatively impact the outcome because it's helpful to choose the right people to lead and coordinate the project. The risk rating is low because once this is set up and decided, it is now up to the system to deliver requirements and specifications (Software Intelligence for Digital Leaders, N.D).

Other Risks:

Risk Category	Risk Factor	Risk Level
Strategic	Misalignment with overall Information Technology Architecture.	High
Technical	Not meeting system's IT (software, hardware, network, and security) requirements/specifications.	Low
Operational	Business case' outlined benefits not met.	Moderate
Project Management	Necessary project resources have not been available.	Moderately High
Organisational Fit	Failure to reengineer business processes.	Moderate
Management	Inadequate communication system.	Moderate
Operational	Lack or no disaster recovery plan.	High
Management	No Risk management process.	High
Strategic	Unclear objectives /Inadequate ERP implementation strategy.	High
Strategic	Inadequate measure to align with Sarbanes-Oxley Act (SOX)	Low
User involvement and training.	Insufficient end-user training.	Moderate
User involvement and training.	Insufficient sensitivity to user resistance.	Moderate
Technical	Incorrect ERP package selection.	High
Project Management	Quality deficiency because of time/cost drivers.	Moderately High
Strategic	The system produced data fails to comply with Data Protection Regulations.	Low

Risk Matrix:

		Risk Severity Matrix				
		Low	Moderate	High	Very High	Extreme
Probability.	Rare					
	Unlikely	team mis-communication			Cost too high for system	
	Possible	Functionality failure	End-user training	No DR plan		Quality deficiency
	Likely	Complex design	Resources shortage	User resistance	DR regular test	
	Extreme					

RISKS AND SDLC:

Risk Category	Risk Factor	Risk Level
Strategic	Misalignment with overall Information Technology Architecture.	High
Technical	Not meeting system's IT (software, hardware, network, and security) requirements/specifications.	Low
Operational	Business case' outlined benefits not met.	Moderate
Project Management	Necessary project resources have not been available.	Moderately High
Organisational Fit	Failure to reengineer business processes.	Moderate
Management	Inadequate communication system.	Moderate
Operational	Lack or no disaster recovery plan.	High
Management	No Risk management process.	High
Strategic	Unclear objectives /Inadequate ERP implementation strategy.	High
Strategic	Inadequate measure to align with Sarbanes-Oxley Act (SOX)	Low
User involvement and training.	Insufficient end-user training.	Moderate
User involvement and training.	Insufficient sensitivity to user resistance.	Moderate
Technical	Incorrect ERP package selection.	High
Project Management	Quality deficiency because of time/cost drivers.	Moderately High
Strategic	The system produced data fails to comply with Data Protection Regulations.	Low

Risk Analysis:

There are two components to risk management, being assessment/analysis and mitigation of risk. Risk analysis identifies, quantifies or qualitatively define risks, and through established evaluation criteria, risks are prioritised (Nieles et al., 2017).

The quantitative risk analysis method estimates the value of the assets using numerical calculation related to each component resulting from the risk assessment (Ramona, 2011).

In qualitative risk analysis, relative values are used as inputs to estimate the impact or the value of the potential loss instead of statistical values. High/often, significant, and low/rare refer to the risk occurrence probability and impact. For classification of the information, words such as general, crucial, critical are used (Sung, 2015).

We chose the qualitative assessment method for the assessment. We considered several factors leading to the choice of qualitative methodology. Firstly, without a comprehensive knowledge of the complete list of assets and the absolute value of the business, it will not be easy to use the quantitative approach since its input are majority numerical. Secondly, the approach simplifies understanding and observation of the level of risk, understanding and implementation of calculation methods are simple. The approach also allows for the determination of areas of greater risk in an abbreviated time and without a more significant expenditure, and analysis is inexpensive and straightforward (Simmons et al., 2017).

DATA ANALYSIS:

The first mechanism of gathering data was sending out a questionnaire to the client a week before engagement. Interviews were also conducted within the first two days of engagement with key decision-makers and end-users. A solution was formulated using the database of risk factors gathered above, the data gathered, the preferences, and the cost benefit analysis below.

COST-BENEFIT ANALYSIS

Cost plays a significant role in most business decisions, especially IT decisions. This report can help management take on particular decisions by clearly outlining all aspects of the system that need to be considered before a new system is introduced. Risk playing a significant factor is also clearly explained in the report, which will thus help management with decision making.

- OPEN SOURCE:

This is a cost-effective, free, publicly accessible system that will be installed and supported by the IT department. Greg Stuart (2019) states that there is a possibility that the open-source software your organisation has hedged their bets on simply goes away. Waking up with no system is a challenge considering that Acme is in dire need of a properly working ERP due to increased demand. The community behind can also close anytime and leave Acme hanging. The risk of hacking and downloading malicious codes is high, considering anyone can update an open-source system. Millions of dollars will be lost, which will make it safer to choose COTS.

- IN-HOUSE:

This is also a no-cost solution that has been developed by a student. Mike Cohn (2018) is of the view that a student programmer does not have to think about work beyond the specification. Just code what was asked for. A student solution also has a high probability of failing to meet specifications, e.g., flexibly managing the supply chain, lack of enough tests, and system failure. Acme needs a solution that has been tried and tested and does work beyond specifications since they anticipate scaling up production.

- COTS:

This solution is a pre-existing solution that is quick to implement, comes with updates and support, development and upgrade costs footed by the manufacturer and can offer Acme more functionality than required. This is a package that Acme needs to be able to adapt to quickly to the changing demand. This package quickly brushes off all problems associated with spreadsheets and offers relief due to spreadsheets being unwieldy. It does come with a total cost of $100k per annum. The truth is, a commercial product is made to work for as many people as possible, and when a product is made for the mass market, it simply cannot satisfy every need of every person (Erin Quilliam, N.D). However, the benefits outweigh the cost; thus, COTS will be the best choice for Acme.

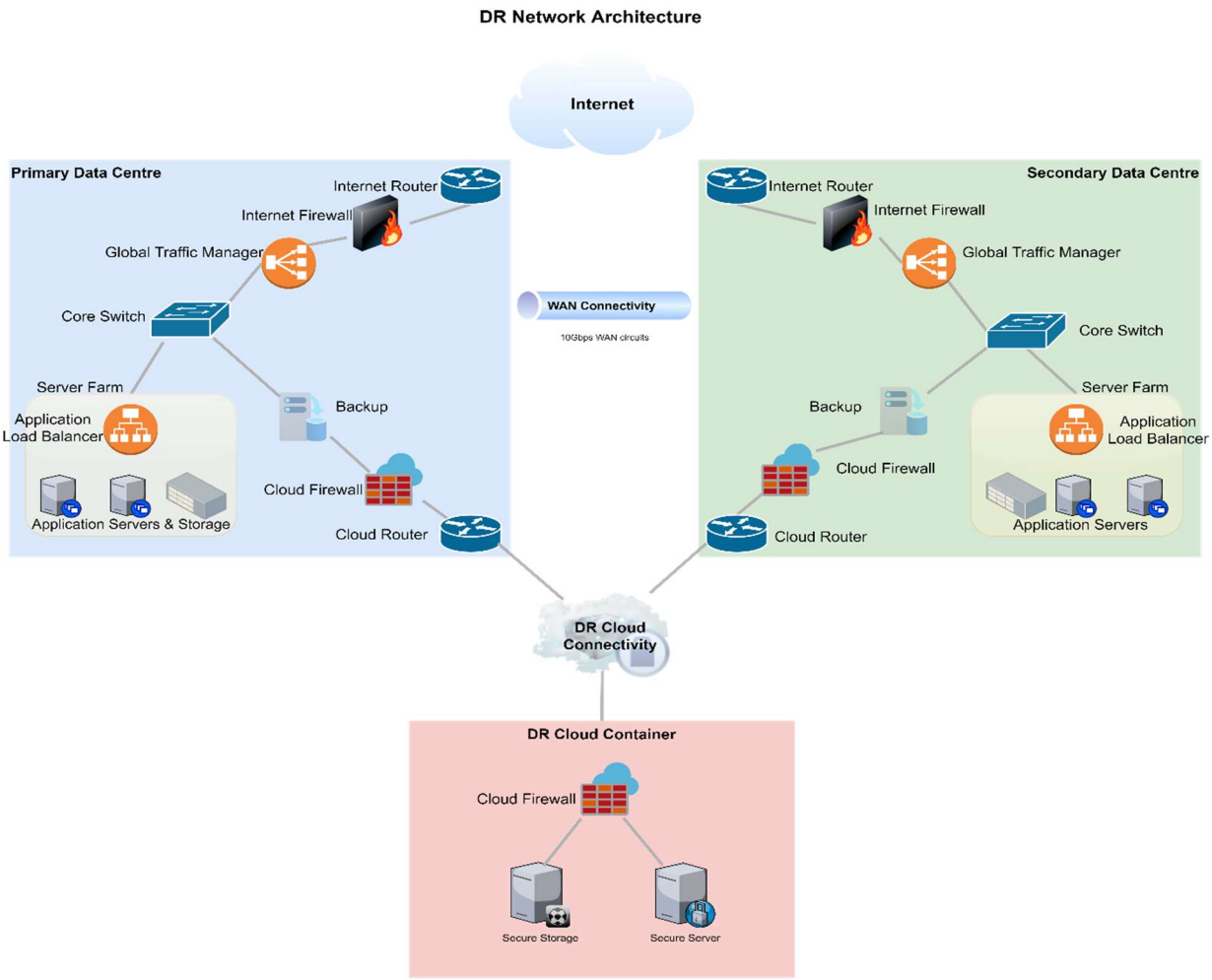
Disaster Recovery Solution Design

Resilience has become the dominant and normative ideology of sustainability more generally and disaster recovery more specifically. Most studies focus on how to achieve resilient recovery. (Sou, 2019)

The disaster recovery solution is essential for any business to have a continuity service. The best practice datacentres are built with full resilience and capabilities. Critical systems and data are replicating and recovering between the data centres and recovery sites.

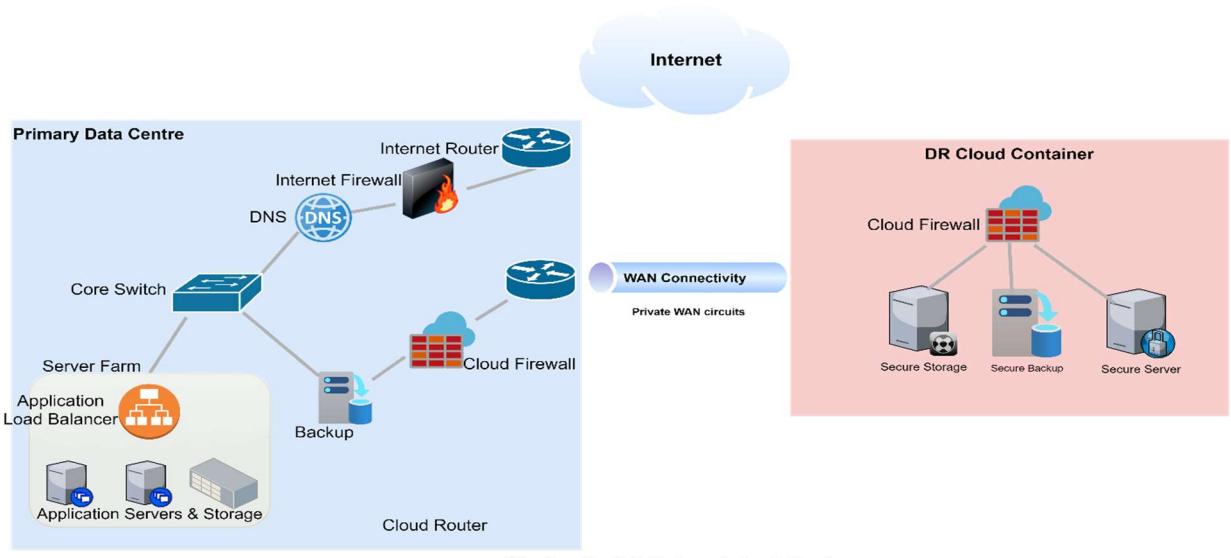
Essential business services are the high point for any DR high-level design. First, the architect-engineer should know the criticality of the business applications and which application data to replicate and back up on recovery point objectives. Then the calculation of how quickly the critical application and systems need to be back up online and running to minimise the business operation impact. The following diagram shows the best resilience design that can any business follow as it provides two active/active or active/standby datacentres with DR sites in the cloud. With the two datacentres design, the business should mirror all infrastructure devices like networks, servers, storage and backups and have the same applications running in both.

Furthermore, the risk management team should make sure any change applies on both sides to avoid any miss-implementation.



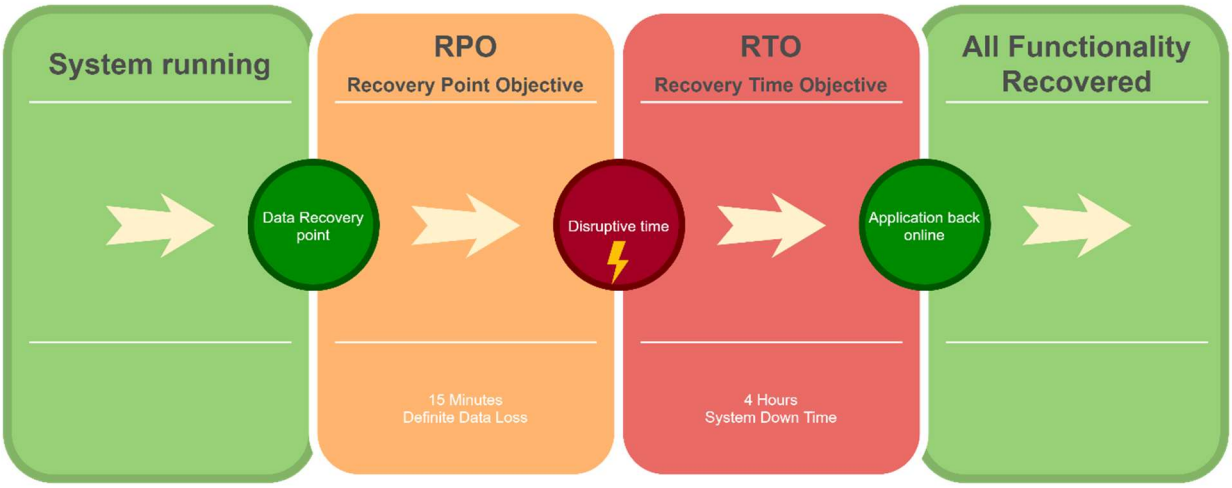
Best Practise Active/Active or Active/Standby DR design

For small/medium businesses that do not need a high resiliency and to control the cost efficiency of the implementation and operation, the following design can show one datacentre with a DR cloud site.



Single site DR Network Architecture

All applications run in the server farm secured zone and save all data in the storage connected to the servers. Automation backup policies are required to run every 15 minutes to back up all the stored data to the backup system. DR backup system has to be in synch with the protected site and replicating the data during the business hours using the private WAN connectivity between the datacentre and the cloud DR site. The challenge for the operation is how to keep the network established between protected and recovery sites all the time. The challenge for the risk management team is how to ensure all IT engineers are replicating the changes on the protected site into the recovery site to avoid any issues when the DR applications have to be put as live services.



Disruptive Event Time Point

As an example scenario about the provided design, if the system goes down at 11:30 a.m., all the data can be recovered from the Dr site at least from 11: 14 a.m., then the RPO is 15 minutes if the IT team is going to bring the applications online on the DR site by checking the backup system, then restore the data to the DR storage and link it to the DR application servers within 4 hours, so the RTO is 4 hours to recover and back all service online.

References :

- Aloini, D., Dulmin, R., & Mininno, V. (2007). Risk management in ERP project introduction: Review of the literature. *Information and Management*, *44*(6), 547–567. https://doi.org/10.1016/j.im.2007.05.004
- Dey, P. K., Clegg, B., & Cheffi, W. (2013). Risk management in enterprise resource planning implementation: A new risk assessment framework. *Production Planning and Control*, *24*(1), 1–14. https://doi.org/10.1080/09537287.2011.597038
- Erin Quilliam (N.D) The complete advantages and disadvantages of off the shelf software. Available from: https://itenterprise.co.uk/off-the-shelf-software-pros-cons/ [Accessed on 12 September 2021]
- Greg Stuart (2019) The pros and cons of open source tools. Available from: https://orangematter.solarwinds.com/2019/02/15/the-pros-and-cons-of-open-source-tools/ [Accessed on 12 September 2021]

- Joint Task Force. (2018). SP 800-037, Rev.2, Risk Management Framework (RMF) for Information Systems and Organisations. *NIST Special Publication - 800 Series*, 183. https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final%0Ahttps://doi.org/10.6028/NIST.SP.800-37r2
- Lopez, C., & Salmeron, J. L. (2011). A framework for classifying risks in ERP maintenance projects. *ICE-B 2011 - Proceedings of the International Conference on e-Business*, 201–204. https://doi.org/10.5220/0003407802010204
- Mike Cohn (2018) The difference between a professional and an amateur. Available from: https://www.mountaingoatsoftware.com/blog/the-difference-between-a-professional-and-an-amateur [Accessed on 12 September 2021]
- Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). NIST Special Publication 800-12 Revision 1 - An introduction to information security. *NIST Special Publication*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf
- Ojala, M., Vilpola, I., & Kouri, I. (2006). Risks in ERP project - Case study of IS/ICT management capability maturity level and risk assessment. *Proceedings of the International Conference on Electronic Business (ICEB)*.
- Ramona, S. E. (2011). Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches. *Chinese Business Review*, *10*(12), 1106–1110. https://doi.org/10.17265/1537-1506/2011.12.002
- Simmons, D. C., Dauwe, R., Gowland, R., Gyenes, Z., King, A. G., Riedstra, D., & Schneiderbauer, S. (2017). Qualitative and quantitative approaches to risk assessment. *Understanding Disaster Risk: Risk Assessment Methodologies and Examples*, 44–130.
- Ready.gov (N.D) Risk assessment. Available from: https://www.ready.gov/risk-assessment [Accessed on 18 September 2021]
- Software Intelligence for Digital Leaders (N.D) Risk Management in Software Development and software Engineering Projects. Available from: https://www.castsoftware.com/research-labs/risk-management-in-software-development-and-software-engineering-projects [Accessed 9 September 2021].
- Sou, G. (2019) 'Sustainable resilience? Disaster recovery and the marginalisation of sociocultural needs and concerns', Progress in Development Studies, 19(2), pp. 144–159. doi: 10.1177/1464993418824192.
- Sung, S. H. (2015). Quantitative and Qualitative Approach for IT Risk Assessment. *Asia-Pacific Journal of Convergent Research Interchange*, *1*(1), 29–35. https://doi.org/10.21742/apjcri.2015.03.04
- Thangamani, G. (2018). Practical Risk Assessment Methodology for ERP Project Implementation. *Journal of Economics, Business and Management*, *6*(3), 84–90. https://doi.org/10.18178/joebm.2018.6.3.555