Risk No.	Risk	Description	Potential Effect	Risk Assessment			Recommendation	Treatment
				Probability	Impact	Risk Level		
COTS (Commercial Off the Shelf) solution								
1	Inadequate support of COTS vendor	The COTS vendor may stop providing support or provide inadequate support either due to incompetency or bankruptcy	Inadequate service quality Security breaches and incidents Non-compliance with regulatory authority Financial loss and reputational damage	3	3	9	Transfer/ Reduce	1. COTS products should be well known with support capabilities from multiple suppliers. 2. Contract should
2	Process risk	The COTS application may require more time than required to understand and integrate business processes	Sustainability of application leading to service degradation	3	2	6	Mitigate	Adopt agile approach for solution delivery which will reduce time to delivery
3	SLAs not meeting agreed-on metrics	Depending on the support model agreed, the vendor could breach the SLA	Not able to provide the agreed-on RTO and RPO	3	3	9	Mitigate	1. Establish metrics for monitoring SLAs. 2. Add indemnification clause for breach of SLA
4	Product obsolescence	Lack of product enhancements and/or product development may get dropped	Inadequate service quality Security breaches and incidents Financial loss and reputational damage Not able to meet organisations strategic objectives	3	3	9	Mitigate	Choose the subscription model. A monthly or yearly subscription model will address the risk of obsolescence
Open-Source solution supported by Internal IT department								
1	Software quality	Open source projects are community-oriented, developed and supported through collaboration. However with	Inadequate service quality Not able to meet strategic objectives	3	3	9	Mitigate	1.Train/upskill niche resrouces. 2. During the planning
2	Sustainability over longer time period	As open-source projects relies on community contributions, if the contributors are not able to keep the commitment, it will lead to a product	Inadequate service quality Security breaches and incidents Not able to meet organisations strategic objectives	3	3	9	Mitigate	Developers should check: 1.No of commits that shows level of activity

3	Copyright infringement	Negligence from coder can potentially allow proprietary code in the product.	Financial loss and reputational damage	3	3	9	Mitigate	Incorporate automated tools to track the usage of open source licenses
4	Software security risks	Open-source vulnerabilities and exploits are made public to everyone once discovered. If there is a	Security breaches and incidents Financial loss and reputational damage	3	4	12	Mitigate	1. Adopt a continuous vulnerability management
In-house developed solution built by a student and supported by Internal IT department								
1	Unrealistic estimated schedule	The solution developed by the student may have unrealistic deadline for completion	Not able to meet organisations strategic objectives	4	2	8	Mitigate	Transfer solution to internal IT dept for development.
2	Lack of adequate skill set	The solution may suffer quality issues and/or not meet the expectations due to a lack of required skill set	Not able to meet organisations strategic objectives Security breaches and incidents Inadequate service quality	4	3	12	Mitigate	Purchase COTS application and adopt agile methodology for quick deployment
3	Incomplete solution	There is a risk of an incomplete solution if the student discontinues the course	Not able to meet organisations strategic objectives	2	3	6	Mitigate	Transfer solution to internal IT dept for development.
4	Lack of upper management involvement	Risk of upper management not being involved with the student	Not able to meet organisations strategic objectives	2	3	6	Mitigate	Month/Quarterly progress meetings to review the progress and risks
5	Insufficient testing	There is a risk of the solution not being tested sufficiently either due to	Security breaches and incidents Inadequate service quality	3	4	12	Mitigate	1. Adopt a continuous vulnerability

The quantitative method uses numerical and statistical techniques to calculate the likelihood and impact of risk and is data-driven and produces statistically reliable results. Given the high degree of uncertainty and insufficient knowledge, a quantitative method will not yield a satisfactory result. Also, reliable historical data is not available for analysis to quantify risk. Qualitative analysis often reflects inputs of business units more accurately than quantitative analysis, and it also captures “soft” risks. Considering the above, we used the qualitative assessment method

Impact Matrix					
	Negligle (1)	**Minor(2)**	**Major(3)**	**Extensive(4)**	**Catastrophic(5)**

Reputation	Contained to industry and insiders locally	Local media coverage and reputation impact	National media coverage and local criticism	Short term international media coverage and business impacting reputational damage	Long term (>1) international attention and lasting reputational damage
Financial	< $100K	< $500K	< $2M	< $5M	< $10M
Health & safety	Minor first aid	Medical treatment incident	Hospitalization/Lost Time Injury (LTI) of multiple persons	Fatal incident up to 5 people	Mass fatalities > 5

Probability Matrix

	Likelihood	**Frequency**	**Percentage Probability**
Very High (5)	Expected to occur in most circumstances	Can happen often in a year	75%+
High (4)	Likely to occur in many circumstances	Expected yearly	50-70%
Medium (3)	May occur but less likely than likely	Once every few years	21-49%
Low (2)	Can occur but unlikely	At least once in 5 years	6-20%
Very low (1)	May occur only in exceptional circumstances	Once in 10 years event	> 5%

Risk Matrix

	Negligle (1)	**Minor(2)**	**Major(3)**	**Extensive(4)**	**Catastrophic(5)**
Very High (5)	Medium	Medium	High	Very High	Very High
High (4)	Low	Medium	High	Very High	Very High
Medium (3)	Low	Medium	Medium	High	Very High
Low (2)	Low	Low	Medium	High	Very High
Very low (1)	Low	Low	Medium	Medium	High

Based on the risk appetite, financial appetite and risk assessment conducted, we recommend procuring the COTS application

References:

. [online] Available at: https://ao.ms/understanding-the-risks-of-commercial-off-the-shelf-software-cots/ [Accessed 22 Mar. 2022].
ailable at: https://snyk.io/learn/risks-of-open-source-software/ [Accessed 22 Mar. 2022].

ww.whitesourcesoftware.com/resources/blog/top-3-open-source-risks-and-how-to-beat-them/ [Accessed 23 Mar. 2022].
ɔs://www.researchgate.net/figure/Top-ten-risks-factors-in-inhouse-outsourced-software-projects_tbl2_319643465 [Accessed 24 Mar. 2022].
tion (2013). CRISC review manual 2014. Rolling Meadows, Ill.: Isaca.