#	Risk	Mitigation	Summary Data						Risk Description			Risk Analysis Result						Risk Response					Risk Indicators	
1	Power Outage	- Provide a UPS for the servers	Risk Assessment	The frequency is very high since the users of the system are students meaning that they are young and that they are more careless in using a computer compared to other type of users. The impact is very low since it would only affect a single student.					Title	Power outage		Likelihood of Scenario	very low	low	moderate	high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	
			Risk Owner	Student					High Level Scenario	Unplanned power outage		Comments on likelihood	People are usually informed of outages, such unplanned outages are rare					Justification	Power is needed in order for the students to perform their tasks					
			Date of Last Risk Assessment						Detailed Scenario	Actor		Impact on productivity	very low	low	moderate	high	very high	Detailed Description of response	Response Action		Completed	Action Plan		
			Due date for update of Risk Assessment							Threat Type	Machine	Comments	By providing a UPS, the servers could start again right after the unplanned outage						Provide generators					
			Risk Category	strategic	project delivery		operational			Event		Impact on competitive advantage	very low	low	moderate	high	very high		UPS					
			Risk Classification	very low	low	moderate	high	very high		Asset	Computer	comments	NA					Overall status of risk action						
			Risk Response	accept	transfer	reduce/mitigate		avoid		Timing	Any time	impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan	none					
									Other Info			comments	NA					Overall status of completed action						
												Overall impacts	very low	low	moderate	high	very high	Major issues with completed response						
												comments	NA											
#	Risk	Mitigation	Summary Data						Risk Description			Risk Analysis Result						Risk Response					Risk Indicators	
2	Unauthorized Access	- Create or provide a two factor authentication so that the actor cannot easily access user's login information through one source only	Risk Assessment	The frequency is moderate since it would depend on how secure the student may be. The impact is low since it would only affect a single student and could only gain his/her information.					Title	Unauthorized Access		Likelihood of Scenario	very low	low	moderate	high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	
			Risk Owner	Any user					High Level Scenario	Student account is accessed by unauthorized user		Comments on likelihood	Depending on how cautious or secured a student is, the likelihood could change					Justification	Login credentials can be known through the user					irregular behavior of user
			Date of Last Risk Assessment						Detailed Scenario	Actor	Human	Impact on productivity	very low	low	moderate	high	very high	Detailed Description of response	Response Action		Completed	Action Plan		
			Due date for update of Risk Assessment							Threat Type	Human	Comments	It would only affect a single student and not the whole system						Access control features					
			Risk Category	strategic	project delivery		operational			Event		Impact on competitive advantage	very low	low	moderate	high	very high		Password change/two factor					
			Risk Classification	very low	low	moderate	high	very high		Asset	Student Information	comments	NA					Overall status of risk action						
			Risk Response	accept	transfer	reduce/mitigate		avoid		Timing		impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan						
									Other Info			comments	NA					Overall status of completed action						
												Overall impacts	very low	low	moderate	high	very high	Major issues with completed response						
												comments	Students, themselves, should be a security measure											
#	Risk	Mitigation	Summary Data						Risk Description			Risk Analysis Result						Risk Response					Risk Indicators	
3	Intrusion	Set standard for passwords. Keep system up-to-date. Use intrusion Prevention System. Back up your data in different places. Keep accounts logged out when not present. Prevent unauthorized people entering the vicinity or server rooms	Risk Assessment	The frequency is low since it is very unlikely for an intrusion to happen in a secure location like DLSU. The impact is high since the intruder may access confidential and very essential data from the system.					Title	Intrusion		Likelihood of Scenario	very low	low	moderate	high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	
			Risk Owner	System administrator					High Level Scenario			Comments on likelihood	DLSU is a secure location					Justification	Unauthorized person in unauthorized location could compromise the system					
			Date of Last Risk Assessment						Detailed Scenario	Actor	Human	Impact on productivity	very low	low	moderate	high	very high	Detailed Description of response	Response Action		Completed	Action Plan		
			Due date for update of Risk Assessment							Threat Type	Human	Comments	Might compromise the system						Use of IPS					
			Risk Category	strategic	project delivery		operational			Event		Impact on competitive advantage	very low	low	moderate	high	very high		Training/protocols to always log out accounts when not in use					
			Risk Classification	very low	low	moderate	high	very high		Asset	System	comments	NA					Overall status of risk action						
			Risk Response	accept	transfer	reduce/mitigate		avoid		Timing		impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan	Cannot completely avoid the problem					
									Other Info			comments	NA					Overall status of completed action						
												Overall impacts	very low	low	moderate	high	very high	Major issues with completed response						
												comments	Could compromise the system but with enough measures, it could be avoided											
#	Risk	Mitigation	Summary Data						Risk Description			Risk Analysis Result						Risk Response					Risk Indicators	
4	Man-in-the-middle attacks	Never connect to open WIFI directly. Make transactions between client and server encrypted. It could involve the use of digital certificates	Risk Assessment	The frequency is moderate since students would use their virtual machines in public areas (with public network connection) less compared than using it in school meaning that there are less chances of them being attacked. The impact is moderate since the intruder may access confidential student/class data.					Title	Man-in-the-middle attacks		Likelihood of Scenario	very low	low	moderate	high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	
			Risk Owner						High Level Scenario	Passwords are retrieved from a user logging in		Comments on likelihood	Students are most of the time connected to the internet so they might come across an open WIFI and just connect with it, hence the likelihood					Justification	Easy to apply					
			Date of Last Risk Assessment						Detailed Scenario	Actor	Users	Impact on productivity	very low	low	moderate	high	very high	Detailed Description of response	Response Action		Completed	Action Plan		
			Due date for update of Risk Assessment							Threat Type	Human	Comments	Limited to the student only											
			Risk Category	strategic	project delivery		operational			Event		Impact on competitive advantage	very low	low	moderate	high	very high							
			Risk Classification	very low	low	moderate	high	very high		Asset	System Data	comments	NA					Overall status of risk action						
			Risk Response	accept	transfer	reduce/mitigate		avoid		Timing		impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan	none					
									Other Info			comments	NA					Overall status of completed action						
												Overall impacts	very low	low	moderate	high	very high	Major issues with completed response						
												comments	Could be avoided if devices will only connect on secure WIFI											
#	Risk	Mitigation	Summary Data						Risk Description			Risk Analysis Result						Risk Response					Risk Indicators	
5	VIrtual Machine Crashing	Backup data in different locations. Save important or crucial files to different locations.	Risk Assessment	The frequency is high or very low depending on what is causing the machine to crash. If it is simple data interruption/corruption, it has a high frequency since it normal for machines to crash because of data interruption. If it is cloud service hacking, it has a very low frequency because cloud services are very secure. The impact is very low or very high depending on what is causing the machine to crash. If it is simple data interruption/corruption, it has a very low impact since it would only affect a single student. If it is a cloud service hacking, it has a very high impact since it means that the whole system would be affected.					Title	VIrtual Machine Crashing		Likelihood of Scenario	very low	low	moderate	high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	

			Risk Owner	Users					High Level Scenario	cloud service hacking		Comments on likelihood	Depends on the cause of the crash					Justification	Using those virtual machines is vital.					Slow virtual machines
			Date of Last Risk Assessment						Detailed Scenario	Actor	Users	Impact on productivity	very low	low	moderate	high	very high	Detailed Description of response	Response Action	Completed	Action Plan			Lags
			Due date for update of Risk Assessment							Threat Type	Machine	Comments	Could simply be solved by restarting but might also be a problem in cloud itself						Back up of data					
			Risk Category	strategic	project delivery	operational				Event		Impact on competitive advantage	very low	low	moderate	high	very high							
			Risk Classification	very low	low	moderate	high	very high		Asset	Computer	comments	NA					Overall status of risk action						
			Risk Response	accept	transfer	reduce/mitigate	avoid			Timing		impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan						
									Other Info			comments	NA					Overall status of completed action						
												Overall impacts	very low	low	moderate	high	very high	Major issues with completed response						
												comments	Depends on the cause of the crash											
#	Risk	Mitigation	Summary Data						Risk Description			Risk Analysis Result						Risk Response					Risk Indicators	
6	Destruction of Cloud Servers	Backup data into your local servers to provide to have a higher chance of restoring your data	Risk Assessment	The frequency is very low since it is very unlikely for a cloud server to be destroyed by nature/accidents. The impact is very high since it means that it would affect the whole system					Title	Destruction of Cloud Servers		Likelihood of Scenario	very low	low	moderate	high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	
			Risk Owner	Users					High Level Scenario	System cannot be accessed		Comments on likelihood	NA					Justification	Servers hold your data, if it crashes your data may be deleted					Cannot access service or data
			Date of Last Risk Assessment						Detailed Scenario	Actor	User/Nature	Impact on productivity	very low	low	moderate	high	very high	Detailed Description of response	Response Action	Completed	Action Plan			
			Due date for update of Risk Assessment							Threat Type	Machine	Comments	Inability to use the system if ever it occured						Use of local servers					
			Risk Category	strategic	project delivery	operational				Event	Servers crash	Impact on competitive advantage	very low	low	moderate	high	very high		Storing data in different locations					
			Risk Classification	very low	low	moderate	high	very high		Asset	Servers	comments	NA					Overall status of risk action						
			Risk Response	accept	transfer	reduce/mitigate	avoid			Timing		impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan	Costly					
									Other Info			comments	NA					Overall status of completed action						
												Overall impacts	very low	low	moderate	high	very high	Major issues with completed response						
												comments	NA											
#	Risk	Mitigation	Summary Data						Risk Description			Risk Analysis Result						Risk Response					Risk Indicators	
7	Permanent Data Loss	Creation of a rule to backup data every now and then. Update your anti-virus software. Maintain hardwares/ clean your PC.	Risk Assessment	The frequency is very low since it is very unlikely for a user to do errors in handling confidential data. The impact is high since it could affect the whole system					Title	Data Loss		Likelihood of Scenario	very low	low	moderate	high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	
			Risk Owner	Users					High Level Scenario	Permanent loss of data		Comments on likelihood	NA					Justification	Possible loss of data should be immediately be addressed and be completely avoided for all information that the system uses is in it					No data is returned
			Date of Last Risk Assessment						Detailed Scenario	Actor	Users/Student	Impact on productivity	very low	low	moderate	high	very high	Detailed Description of response	Response Action	Completed	Action Plan			
			Due date for update of Risk Assessment							Threat Type	Human, Machine	Comments	Could affect the whole system						Backup					
			Risk Category	strategic	project delivery	operational				Event		Impact on competitive advantage	very low	low	moderate	high	very high							
			Risk Classification	very low	low	moderate	high	very high		Asset	Database, System data	comments	NA					Overall status of risk action						
			Risk Response	accept	transfer	reduce/mitigate	avoid			Timing		impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan	Need for additional storage space					
									Other Info			comments	NA					Overall status of completed action						
												Overall impacts	very low	low	moderate	high	very high	Major issues with completed response						
												comments	Overall loss of data will make all previous information inaccessible											
#	Risk	Mitigation	Summary Data						Risk Description			Risk Analysis Result						Risk Response					Risk Indicators	
8	Data Leakage	Encrypt every data or transaction that are deemed sensitive such as passwords.	Risk Assessment	The frequency is moderate since it is possible for students to leak important data especially if they are accessing the data in a public location. It has moderate impact since if the leaked data is essential, it could affect the whole system and could lead to more severe attacks					Title	Data Leakage		Likelihood of Scenario	very low	low	moderate	high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	
			Risk Owner	Users					High Level Scenario	System administrator credentials are leaked		Comments on likelihood	Could be leaked in public					Justification	Sensitive information might be leaked					Users are accessed in uncommon places
			Date of Last Risk Assessment						Detailed Scenario	Actor	Human	Impact on productivity	very low	low	moderate	high	very high	Detailed Description of response	Response Action	Completed	Action Plan			
			Due date for update of Risk Assessment							Threat Type	Human	Comments	Could lead to potential attacks						Encryption of data					
			Risk Category	strategic	project delivery	operational				Event	Unauthorized user accessing administrator	Impact on competitive advantage	very low	low	moderate	high	very high							
			Risk Classification	very low	low	moderate	high	very high		Asset	Database, System data	comments	NA					Overall status of risk action						
			Risk Response	accept	transfer	reduce/mitigate	avoid			Timing		impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan	none					
									Other Info			comments	NA					Overall status of completed action						
												Overall impacts	very low	low	moderate	high	very high	Major issues with completed response						
												comments	If accessing the system in public unavoidable, make sure that your data/information is secured											
#	Risk	Mitigation	Summary Data						Risk Description			Risk Analysis Result						Risk Response					Risk Indicators	
9	Denial of Service	Set up the firewall.Provide a device or service that checks inbound traffic before it reaches the firewall. Check	Risk Assessment	The frequency is moderate since students would use their virtual machines in public areas (with public network connection) less compared than using it in school meaning that there are less chances of them being attacked. The impact is high because it could affect the whole system and could even stop its processes.					Title	Denial of Service		Likelihood of Scenario	very low	low	moderate	high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	

		reaches the firewall. Check for signs of attacks. Know what or who to contact in case of an attack.	Risk Owner	Students, System Administrator					High Level Scenario	System administrator unable to access the system		Comments on likelihood	Could be brought by technical problems					Justification	Deny of access to the system is a requirement				slow connection	
			Date of Last Risk Assessment						Detailed Scenario	Actor	Human	Impact on productivity	very low	low	moderate	high	very high	Detailed Description of response	Response Action	Completed	Action Plan		Repeated refresh won't help	
			Due date for update of Risk Assessment							Threat Type	Machine	Comments	It involves the accessing the system						Setting up a firewall					
			Risk Category	strategic	project delivery		operational			Event		Impact on competitive advantage	very low	low	moderate	high	very high		Device or service to detect inbound traffic					
			Risk Classification	very low	low	moderate	high	very high		Asset	System	comments	NA					Overall status of risk action						
			Risk Response	accept	transfer	reduce/mitigate		avoid		Timing	Maintenance/ Any	impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan	NA					
									Other Info			comments	NA					Overall status of completed action						
												Overall impacts	very low	low	moderate	high	very high	Major issues with completed response						
												comments												