- 1	Risk	Mitigation	Summary Data Ri						Risk Description						Risk Response						ors	
	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.				are T more users. student.	Title	Power or	itage	Risk Analysis Result Likelihood of Scenario	very low low	moderate hig	h very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk		
			Risk Owner	ner Student			H	High Level Scenario	Unplannoutage	ed power	Comments on likelihood	People are usually unplanned outage		ges, such	Justification		needed in their tasks	order for the stud	ents to		T	
			Date of Last Risk Assessment				0	Detailed Scenario	Actor		Impact on productivity	very low low	moderate hig	h very high	Detailed Description of response	Respons		Completed	Action Plan		T	
			Due date for update of Risk						Threat	Machine	Comments	By providing a UPS		d start again		Provide	generators				+	
			Assessment Risk Category	strategic	project delivery	operational			Type Event		Impact on	right after the unp	moderate hig	h very high		ı	JPS				+	
			0.1.01.15.11	ļ .							competitive advantage										퇶	
			Risk Classification Risk Response	very low accept	transfer reduce/m		ery high void			Computer Any time	comments impact on legal	NA very low low	moderate hig	h very high	Overall status of risk action Major Issues with risk action plan			none			\pm	
								Other Info			comments Overall impacts	NA very low low	moderate hig	h verv high	Overall status of completed action Major issues with completed response	ie.					+	
	Risk	Mitigation	Summary Data				D	Risk Descripti	ion		comments Risk Analysis Result	NA		, , ,	Risk Response					Risk Indicato	1	
	Unauthorized Access	Create or provide a two factor authentication so that the actor cannot easily	Risk Assessment	the student	ncy is moderate since it wou i may be. The impact is low ent and could only gain his/h	since it would only	v secure T	Title	-	rized Access	Likelihood of Scenario	very low low	moderate hig	h very high		accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	Ť	
		access user's login information through one	Risk Owner	Any user				High Level Scenario	accessed		Comments on likelihood	Depending on how the likelihood coul		red a student is,	Justification	Login cre	edentials ca	in be known throu	lgh the	TOT THIS FISK	in	
		source only	Date of Last Risk Assessment					Detailed Scenario	Actor	ized user Human	Impact on productivity	very low low	moderate hig	h very high	Detailed Description of response	Respons	e Action	Completed	Action Plan		of	
			Due date for update of Risk Assessment	e of Risk					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 hig	h very high	ħ	Password change/two factor					T	
			Risk Classification	very low low moderate accept transfer reduce/mit		high very high			Asset	Student Information	comments	NA .			Overall status of risk action						Ī	
			Risk Response	accept	transfer reduce/m	iitigate av		Other Info	Timing		impact on legal comments	very low low NA	moderate hig	n very nigr	Major Issues with risk action plan Overall status of completed action						+	
											Overall impacts comments	very low low Students, themselv	moderate hig		Major issues with completed respons	ie					+	
	Risk Intrusion	Mitigation Set standard for passwords.	Summary Data Risk Assessment	Th 6	and a law along the control	Illiani, dan an Internal	_	Risk Descripti Title	ion Intrusion		Risk Analysis Result Likelihood of		moderate hig		Risk Response Response for this risk	accept	transfer	reduce/mitigate	avoid	Risk Indicato Key risks	rs	
ľ	in Gaon	Keep system up-to-date. Use intrusion Prevention System. Back up your data	Risk Owner	the intruder	ncy is low since it is very un a secure location like DLSU. r may access confidential ar dministrator	The impact is high the description of very essential discription	h since lata from	High Level	intrusion		Scenario Comments on	very low low DLSU is a secure lo		h very high	Justification			on in unauthorized		indicators for this risk		
		in different places. Keep accounts logged out when not present. Prevent unauthorized people entering the vicinity or server rooms		System a	ummstrator		s	Scenario		T	likelihood					could co		1				
			Date of Last Risk Assessment					Scenario		Human	Impact on productivity	very low low Might compromise	moderate hig	h very high	Detailed Description of response	Respons	e Action of IPS	Completed	Action Plan		1	
			Assessment Risk Category	strategic	project delivery	operational			Type	numan	Impact on	very low low	moderate hig	h very high	1	Training/protocol:					+	
											competitive advantage					accounts	ys log out when not use					
			Risk Classification Risk Response	very low	low moderate transfer reduce/m		ery high void		Asset System Timing 0		comments impact on legal	NA very low low	moderate hig	h very high	Overall status of risk action Major Issues with risk action plan	Can	not comple	etely avoid the nro	hlem		Ŧ	
-			NO NESPONSE	иссерс	, and preduce/iii	- Jane		Other Info			comments	NA		Overall status of completed action						#		
											Overall impacts comments	very low low Could compromise	moderate hig the system but w		igh Major issues with completed response						t	
-	Risk	Mitigation	Summary Data				R	Risk Descripti	rintion		Risk Analysis Result	measures, it could be avoided			Risk Response					Risk Indicato	Indicators	
	Man-in-the-middle attacks	Never connect to open WIFI directly. Make transactions between client and server		machines is	ncy is moderate since stude n public areas (with public n than using it in school mean them being attacked. The ir	atwork connection	ir virtual T	Title		he-middle	Likelihood of Scenario	very low low	moderate hig	h very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk	Ī	
		encrypted. It could involve the use of digital certificates	compared from using it in school meaning that there are less chances of them being attacked. The impact is moderate since the intruder may access confidential studenticlass data. RISK Owner					High Level Scenario		ds are retrieved ser logging in	Comments on likelihood	Students are most internet so they m and just connect w	ght come across	an open WIFI	Justification	Easy to a	ipply				†	
			Date of Last Risk					Detailed	Actor	Users	Impact on	very low low	moderate hig		Detailed Description of response	Respons	e Action	Completed	Action		†	
			Assessment Due date for update of Risk				s	Scenario	Threat	Human	productivity Comments	Limited to the stud	ent only		-				Plan		t	
			Assessment Risk Category	strategic	project delivery	operational			Type Event		Impact on competitive	very low low	moderate hig	h very high							+	
			Risk Classification	very low	low moderate	high ve	ery high		Asset	System Data	advantage comments	NA			Overall status of risk action			1			+	
			Risk Response	accept	transfer reduce/m		void	Other Info	Timing		impact on legal comments	very low low NA	moderate hig	h very high	Major Issues with risk action plan Overall status of completed action			none			Ŧ	
								Julef IIII0			Overall impacts	very low low	moderate hig		Major issues with completed respons	ie					+	
											comments	Could be avoided i secure WIFI	devices will only	connect on								
_		Mitigation	Summary Data 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,					Risk Descripti		la abila a	Risk Analysis Result	t			Risk Response	Invested.	Risk Indicato	rs				
	VIrtual Machine Crashing	Backup data in different locations. Save important or crucial files to different locations.	KISK ASSESSMENT	has a high because of very low fre impact is we machine to	ney is might of very low depe- e to crash. If it is simple data frequency since it normal fo data interruption. If it is close equency because cloud servery low or very high dependi crash. If it is simple data int impact since it would only all vice hacking, it has a very hole ole system would be affecte	r machines to cras ud service hacking, rices are very secu ing on what is caus terruption/corruptio	sh p, it has a ure. The sing the on, it has	Title	Virtual M Crashing		Likelihood of Scenario	very low low	moderate hig	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks indicators for this risk		

			Risk Owner	Users		High Level Scenario	cloud se	rvice hacking	Comments on likelihood	Depends o	on the ca	use of the crash		Justification	Using the	ose virtual	machines is vital.			Slow virtual machin s	
			Date of Last Risk Assessment Due date for update of Risk				Detailed Scenario	Actor Threat	Users Machine	Impact on productivity Comments	very low Could sim		moderate high ved by restarting but r		Detailed Description of response	Respons Back u	e Action	Completed	Action Plan		Lags
			Assessment Risk Category	strategic	project delivery	operational		Type Event		Impact on competitive	be a probl very low	low	moderate high	very high							
			Risk Classification Risk Response	very low accept	low moderate transfer reduce/m		gh Other Info	Asset Timing	Computer	advantage comments impact on legal comments	NA very low NA	low	moderate high	very high	Overall status of risk action Major Issues with risk action plan Overall status of completed action						
		-								Overall impacts comments	very low		moderate high use of the crash	very high	Major issues with completed response						
	Risk	Mitigation	Summary Data				Risk Descript	ion		Risk Analysis Result		on the car	ise of the crash		Risk Response					Risk Indicato	ors
	Destruction of Cloud Servers	Backup data into your local servers to provide to have a higher chance of restoring	Risk Assessment		ncy is very low since it is ve destroyed by nature/accid t means that it would affect	ry unlikely for a cloud ents. The impact is very the whole system	Title	Servers	ion of Cloud	Likelihood of Scenario		low	moderate high	very high	Response for this risk	accept	transfer			Key risks indicators for this risk	
		your data	Risk Owner	Users			High Level Scenario	System of accessed	annot be	Comments on likelihood	NA				Justification	Servers I may be o		data, if it crashes yo	our data		Canno access service or dat
			Date of Last Risk Assessment				Detailed Scenario	Actor Threat Type Event	User/Nature	Impact on productivity	very low	low	moderate high		Detailed Description of response	Respons		Completed	Action Plan		
			Due date for update of Risk Assessment						Machine	Impact on competitive advantage	Inability to	use the	system if ever it occur	ed		Use of lo	ocal servers	S			
			Risk Category	strategic	project delivery	operational			Servers crash		very low	low	moderate high	very high		Storin; differen	g data in nt locations				
			Risk Classification	very low			gh	Asset	Servers	comments	NA				Overall status of risk action			<u> </u>			
			Risk Response	accept	transfer reduce/m	itigate avoid	Other Info	Timing		impact on legal comments	very low NA	low	moderate high		Major Issues with risk action plan Overall status of completed action			Costly			
										Overall impacts	very low	low	moderate high	very high	Major issues with completed response						
	Risk	Mitigation	Summary Data				Risk Descript	ion		comments Risk Analysis Result	NA				Risk Response					Risk Indicato	ors
	Permanent Data Loss	Creation of a rule to backup		The frequent errors in han	ncy is very low since it is ve ndling confidential data. Th	ry unlikely for a user to do e impact is high since it	° Title	Data Los	s	Likelihood of	very low	low	moderate high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks	
		data every now and then. Update your anti-virus software. Maintain	Risk Owner	Users	the whole system		High Level	Permane	ent loss of data	Scenario Comments on	NA				Justification			a should be immed		indicators for this risk	No dat
		hardwares/ clean your PC.	Date of Last Risk				Scenario Detailed	Actor	Users/Student	likelihood	very low	low	moderate high	very high	Detailed Description of response	informat	ed and be o tion that the e Action	completely avoided se system uses is in Completed	d for all it Action		is return
			Assessment				Scenario		Human.	productivity Comments	.,.		nole system	very mgn	Detailed Description of response			Completed	Plan		
			Due date for update of Risk Assessment					Threat Type	Machine	Comments	Could affe	ct the wr	iole 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 hig	gh	Asset	Database, System data	comments	NA				Overall status of risk action						
			Risk Response	accept transfer reduce/mitigate avoid		Other Info	Timing	System data	impact on legal comments	very low	low	moderate high	very high	Major Issues with risk action plan Overall status of completed action	N	leed for ad	ditional storage sp	ace			
		-								Overall impacts comments	very low low moderate high Overall loss of data will make all previous			very high	Major issues with completed response	ise					
											informatio										
	Risk Data Leakage	Mitigation Encrypt every data or	Summary Data Risk Assessment	The frequen	ncv is moderate since it is p	ossible for students to lea	Risk Descript ak Title	Data Lea	kana	Risk Analysis Result Likelihood of	very low	low	moderate high	yeny high	Risk Response Response for this risk	accept	transfer	reduce/mitigate	avoid	Risk Indicato Key risks	ors
	Data Leakage	transaction that are deemed sensitive such as passwords.		important da location. It hi essential, it o severe attac	ata especially if they are ac has moderate impact since could affect the whole syst cks	cessing the data in a pub if the leaked data is em and could lead to mor	olic	Data Leakage		Scenario			very mgn	Response for this risk	ассерс	transier	reduce/ilitigate	avoiu	indicators for this risk		
			Risk Owner	Users			High Level Scenario		idministrator als are leaked	Comments on likelihood	Could be I	eaked in	public		Justification	Sensitive	e informati	on might be leaked	d		Users are acces in uncor on place
			Date of Last Risk Assessment				Detailed Scenario	Actor	Human	Impact on productivity	very low	low	moderate high	very high	Detailed Description of response	Respons	e Action	Completed	Action		T
			Due date for update of Risk				acenario	Threat	Human	Comments	Could lead	to poter	ntial attacks		1	Encrypt	ion of data	1	riail		
			Assessment Risk Category	strategic	project delivery	operational		Type Event	Unauthorized	Impact on	very low	low	moderate high	very high							-
									user accessing administrator	competitive advantage	NA NA			14.78							
			Risk Classification	very low			5''	Asset	Database, System data	comments					Overall status of risk action						
			Risk Response	accept	transfer reduce/m	itigate avoid	Oth !-/	Timing		impact on legal	very low	low	moderate high		Major Issues with risk action plan			none			1
							Other Info			Comments Overall impacts	NA very low	low	moderate high	very high	Overall status of completed action Major issues with completed response						\perp
]								comments	If accessin	g the sys	tem in public unavoida	ble, make							
	Risk	Mitigation	Summary Data				Risk Descript	ion		Risk Analysis Result		your data	/information is secure	u	Risk Response					Risk Indicato	ors
	Denial of Service	Set up the firewall.Provide a	Risk Assessment	The frequent	ncy is moderate since stude n public areas (with public n han using it in school mean	nts would use their virtua etwork connection) less	^{Bl} Title	Denial of	Service	Likelihood of	very low	low	moderate high	very high	Response for this risk	accept	transfer	reduce/mitigate	avoid	Key risks	
		device or service that checks	1	1		land the state of the same times		1		Scenario					l .	1	1			indicators	1

	of attacks, Know	Risk Owner	Students, System Administrator					High Level	el System administrator		Comments on	Could be brought by technical problems					Justification	Deny of access to th	slow		
	what or who to contact in									access the	ccess the likelihood								conn		
								system											on		
case of all	II attack.	Date of Last Risk						Detailed	Actor	Human	Impact on	very low	low	moderate	high	very high	Detailed Description of response	Response Action	Completed	Action	Repe
		Assessment						Scenario			productivity									Plan	d re
																				1 1	wo
																					he
	1	Due date for update of Risk							Threat	Machine	Comments	It involves	It involves the accessing the system				Setting up a			Т	
		Assessment						Type								firewall		1 1			
	F	Risk Category	strategic	project de	elivery	operationa		l	Event		Impact on	very low	low	moderate	high	very high		Device or service to			Т
											competitive							detect inbound		1 1	
											advantage							traffic		1 1	
	F	Risk Classification	very low	low	moderate	high	ery high		Asset	System	comments	NA					Overall status of risk action				Т
	F	Risk Response	accept	transfer	reduce/mi	tigate	void	1	Timing	Maintenance/	impact on legal	very low	low	moderate	high	very high	Major Issues with risk action plan		NA		Т
		·								Any					'						
				•				Other Info			comments	NA			•		Overall status of completed action				Т
								1			Overall impacts	very low	low	moderate	high	very high	Major issues with completed response				Т
											comments							•			Т