INFSEC3 Project Specifications

Scenario:

Cloud computing has become an accepted practice both on a personal level and at an enterprise level. Certain industries would be more suitable than others and some would be early adopters but generally cloud is here to stay. Cloud computing has historically been classified into 3 types namely Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Our main focus would be IaaS in the form of OpenStack. OpenStack is an open-source cloud computing platform for public and private clouds. The difference between a cloud computing platform as opposed to the traditional virtualization is the concept of utility and elasticity as well as self-service abilities that are not present on traditional virtualization technologies.

Currently, the College of Computer Studies of De La Salle University, thru the efforts of a BSIT capstone project is investigating the potential as well as issues that could arise of deploying and making use of such technologies for an educational institution. The initial use case has been determined to revolve around the needs of the BSIT degree program from the student's entry all the way to when they graduate from the degree. With respect to this vision, the following are the envisioned possible detailed use cases of the project:

1. The ability to provide each and every student their own virtual computer that can be used exclusively without worry of another student messing with the configuration. This virtual computer can also be managed by the student directly in terms of setting up applications (administrator rights), and performing shutdowns and reboots.
2. The student is also allowed to create backups of their computer called snapshots so as to be able to recover from erroneous software installations or configuration changes or any form of corruption of data.
3. Each course is to be given its own virtual image template that a student in the course can create an instance of to be able to have all the resource requirements of the course already pre-configured and ready to use in a lab condition or class. This also removes the requirement from the student to acquire or procure expensive laptops for academic use.
4. With respect to #3 requirement, the software requirements could range from something as simple as a C program compiler all the way to something as complicated as developing mobile applications for both iOS and Android and integration with enterprise tools and applications.
5. There are around 1600 students in terms of population for the College of Computer Studies. For the BSIT it would be estimated at around 400. As such the system should be able to handle the different workload as well as use cases such as a mix of lab work and home work.
6. The system is accessible publicly to allow the student to be able to work at home and continue their projects.
7. Other tools such as project management tools would also be installed within the cloud infrastructure in order to assist or facilitate the work of the various courses and projects.
8. Research projects from Cite4D or capstone projects from BSIT that may require actual deployment for user acceptance testing would also be incorporated into the cloud infrastructure.
9. Given the eventual usage patterns, it is of utmost importance that the resiliency of the infrastructure be carefully designed and configured as this could become a single point of failure for the entire program.
10. Although the services are mostly self-serviced by the end users, it is important that the system allow the faculty member to have control over certain student machine instances.
11. The system administrator should also have control over management and recovery of all instances within the system

Requirements:

1. Given the requirements and use cases as stated, identify risks that could come from technology factors and other factors such as human and environment factors.
    a. Create a complete list of assets that needs to be protected or is susceptible to security risks
    b. Conduct a vulnerability scan on the infrastructure setup to help or aid in the identification of risks.
    c. Conduct a threat landscape analysis to assist in the identification of threats.
    d. Create a RACI chart based on each of the use cases as defined earlier, please expound on each with respect to specific commands or actions that can be conducted

2. Conduct a risk assessment on each of the identified risks and provide justifications on why the ratings are given as such. Use the following definitions for the frequency and impact levels.

Frequency Level	Description
Very High (5)	Potential to occur between every day to every week
High (4)	Potential to occur between every other week to every month
Moderate (3)	Potential to occur every 3 months to a term
Low (2)	Potential to occur at most twice a year
Very Low (1)	Potential to occur at most once a year or less

Impact Level	Description
Very High (5)	Potential damage to the majority or entire system causing catastrophic failure that would require more than 1 week to recover
High (4)	Potential damage to the system causing general system failure that can last up to 3 days
Moderate (3)	Potential damage that can shut down the system for the day
Low (2)	Potential damage that can be isolated to specific classes
Very Low (1)	Potential damage that would only affect specific students and would only require reboots of the instance as an example solution

Risk Acceptance

Freq\Impact	Very High	High	Moderate	Low	Very Low
Very High	🟥	🟥	🟥	🟨	🟨
High	🟥	🟥	🟨	🟨	🟩
Moderate	🟥	🟨	🟨	🟩	🟩
Low	🟨	🟨	🟩	🟩	🟩
Very Low	🟨	🟩	🟩	🟩	🟩

Rating	Possible Action
🟩	Acceptable Risk
🟨	Mitigate Risk
🟥	Mitigate/Transfer/Avoid

3. Recommend risk mitigation efforts that would involve specific solutions and technologies as well as potential procedures on how they are to be applied to mitigate the risk. The mitigation can also be procedural not just technical but the procedure should be something that can be monitored and audited.
4. Use the Risk Registry Form in to document all your results. The output should also be demonstrated or justified.
5. Risk mitigation efforts will be assessed with respect to their applicability and appropriateness as well as their feasibility to be implemented.
6. Document how risk monitoring can take place and justify the new risk rating after the control has been applied.
7. Document KRIs or signs on which the risk level assessed is about to be affected or change that would necessitate another round of identification, assessment for the current risk in question.
8. Develop a business continuity plan for the OpenStack deployment to include:
    a. Discussion on the escalation levels leading to the activation of business continuity
    b. Discussion on the timing and events on when business continuity will be activated
    c. Discussion on the infrastructure and architecture setup to support business continuity
    d. Discussion on the roles of students and faculty in support of business continuity
    e. Discussion on the technology requirements to support business continuity
    f. Discussion on the potential cases for prolonged downtime and activation of business continuity
    g. Discussion on the proposed level of acceptable capacity under a business continuity situation

Rubric:

Aspect	Exceeds Expectation	Meets Expectation	Below Expectation	Not Acceptable
Understand the relationship of information security and risk management.	Ability to identify information security related risks that cover all of the use cases and requirements and are properly justified with details	Ability to identify information security related risks that cover 70% of the use cases and requirements and are justified properly with details	Ability to identify information security related risks that cover less than 50% of the use cases and requirements and are well justified	Unable to justify identified risks or was only able to identify risks for below 50% of the identified use cases and requirements
Understand the fundamental of risk assessment techniques;	Ability to properly rate all of the identified risk in terms of their levels	Ability to properly rate 70% of all the identified risks in terms of levels	Ability to properly rate 50% of all identified risks in terms of levels	Unable to rate properly at least 50% of all identified risks in terms of levels
Understand, evaluate, and risk mitigation strategies	Ability to properly provide mitigation strategies to all unacceptable risks	Ability to properly provide mitigation strategies to 70% of unacceptable risks	Ability to properly provide mitigation strategies to 50% of unacceptable risks	Inability to properly provide mitigation strategies to 50% of unacceptable risks
Understand how to implement disaster recovery plan;	Ability to identify the procedures and tools needed to ensure continuity of business for all use cases and requirements	Ability to identify the procedures and tools needed to ensure continuity of business for 70% of use cases and requirements	Ability to identify the procedures and tools needed to ensure continuity of business for 50% of use cases and requirements	Inability to identify the procedures and tools needed to ensure continuity of business for 50% of use cases and requirements
Documentation	Was able to develop appropriate and accurate documentation for all phases of the life cycle.	Was able to develop appropriate and accurate documentation for most phases of the life cycle.	Was able to develop appropriate and accurate documentation for half phases of the life cycle.	Was not able to develop appropriate and accurate documentation for all phases of the life cycle.
Peer Evaluation	Was able to get good evaluation for 90% of the population.	Was able to get good evaluation for 70% of the population.	Was able to get good evaluation for 50% of the population.	Was able to get good evaluation for 30% of the population.

Risk Registry Form

Summary Data

Risk Statement					
Risk Owner					
Date of Last Risk Assessment					
Due date for update of Risk Assessment					
Risk Category	□Strategic	□Project Delivery	□Operational		
Risk classification (copied from risk analysis/assessment result)	□Very Low	□Low	□Moderate	□High	□Very High
Risk Response	□ Accept	□Transfer	□Reduce/Mitigate	□Avoid	

Risk Description

Title		
High level scenario		
Detailed Scenario	Actor	
	Threat Type	
	Event	
	Asset	
	Timing	
Other Info		

Risk Analysis Result

Likelihood of Scenario	□Very Low	□Low	□Moderate	□High	□Very High
Comments on Likelihood					
Impact on Productivity	□Very Low	□Low	□Moderate	□High	□Very High
Comments					
Cost of Response	□Very Low	□Low	□Moderate	□High	□Very High
Comments					
Impact on Competitive Advantage	□Very Low	□Low	□Moderate	□High	□Very High

Comments					
Impact on Legal	□Very Low	□Low	□Moderate	□High	□Very High
Comments					
Overall Impact	□Very Low	□Low	□Moderate	□High	□Very High
Comments					
Risk Response					
Response for this risk	□ Accept	□Transfer	□Reduce/Mitigate	□Avoid	
Justification					
Detailed description of response	Response Action	Completed	Action Plan		
	1.	□	□		
	2.	□	□		
Overall status of risk action plan					
Major issues with risk action plan					
Overall status of completed response					
Major issues with completed response					
Risk Indicators					
Key Risk Indicators for this risk					