It risk managment

Technology, Information Technology

Assignment: I. T Risk Management Question Hot Site: Hot site is a disaster recovery service and facility that looks into the organization data bases setup. A hot site consists of all the equipment required by the enterprise for performing operations, that include office space, furniture, and other computer equipment. The enterprise carries all the data to hot site in case of inoperable functioning . Hot site is a backup and carbon copy with real time synchronization intact. In case of any disruption the hot site serves for relocation. Hot sites are more useful and widely in use in organizations dealing with financial handling, E-commerce facility providers. Cold Site: A cold site is a disaster recovery service that serves as backup but the customers are needed to provide and install all the equipment needed for performing of operations. It provides physical space for recovery operation. Unlike hot site, it doesn't include hardware setup. It is less costly, however takes time in getting into function . Monthly service charges are charged for performing cold and hot site backup Alternate Site: A location other than the normal facility used to perform critical business functions in the event of disaster occurrence. Alternate site serves as plan B, it is termed as any facility that ensures smooth working despite the breakdown of original setup. Alternate site should be in place prior to any disaster occurrence. Several factors are to be considered in installing and setting up of an alternate site . It must be in accord with the ongoing processes that takes place during the normal activities during routine work. Several options can be created for alternate solution, one of them is to use a software based solution that routes the information to all essential components, and it must contain storage controllers that look into data transfer on basis of volume. Question

#2: Self test and evaluation can be grouped in to categories like software, hardware, and tools and they are done so for ease of use and handling. When grouped together it is easy to perform Verification, validation and certification of software packages. Grouping helps in controlled data program execution, mapping and hardware maintenance. The grouping further helps in understanding the Flow charts and ensuring that the testing and evaluation is performed according to the need of setup. Grouping helps in dealing with similar items by placing them in similar facility . Question # 3: Comprehensive testing takes into account all the considerations that are important for the proper working of a system. It would look into the maintenance, installation , load balancing, regression and reliability testing. Comprehensive testing further looks into the overall environment that is suitable for proper installation and compatibility with the hardware equipment and sees if the tools and software being provided are operable with the existing setup. Comprehensive testing would further ensure that the right kind of personnel are deployed at the right station of system who have sufficient enough knowledge of the equipment or the software that is under use Question # 4: The system testing can be performed in different ways depending on conditions and requirements. It could be based on the specifications or behavior and help determine the strength of software and hardware available. The abbreviated system testing is usually performed without documentation, it is sort of least formal testing conducted, and advantage of abbreviated system testing is, immediate detection of errors in system. Comprehensive testing on other hand includes the performance test, compatibility test, error handling test, and is in documented version, accessibility test also falls under comprehensive testing and it checks for compliance with other systems and setups Question # 5: Risk assessment is the process of identifying and exposing the factors that may pose a threat to the proper working and achievement of end product. It is to mitigate the chances of occurrence of a failure. Risk assessment helps understanding and comprehending factors like potential loss that might occur due to failure and the magnitude of impact. A proper framework should be developed in assessing the risk. Any system that is in contact with external environment is bound to risks and therefore would require proper risk assessment. Risk assessment helps not only in saving the time that might be taken in case of down time of a system but also the resources that might be used in order to make the setup functional again. Question 6: ST&E (Security Testing and Evaluation) Security testing in general is the process of determining information system is effective in protecting the data . Security testing and evaluation leads to better security in information technology products and systems. It exerts a positive effect on overall system including the operational envirment, specifications. ST&E are effective in two ways. firstly, identification of errors and vulnerabilities , secondly a rigorous evaluation which helps in reducing the chances of failure in future. Further ST&E addresses security requirements and their basis. Security testing and evaluation involves activies like configuration management, delivery and operation, high level security design, guidance document . Question # 7: Contingency Plan: The prime purpose of contingency plan is to have a backup in case of disaster and dysfunction. It is the existence of an alternate plan or location that could be used in event of disaster , emergency and system failure. Any system exposed to outside world will have some sort of risk associated with it . they are performed to minimize the risk to minimum. Contingency can be in form of network mapping, vulnerability scanning, integrity and configuration checking. The primary reason is to identify potential vulnerabilities and repair them prior to any disorder. Contingency plan involves assigning virtual machines and create protection groups that will ensure proper working of virtual machines in case of failure. Few disaster recovery services offer self backup plan, in those cases complete contingency plan is not necessary Question # 8: Even if risk assessment is completed, performing contingency planning and system testing is advisable because it serves as second tier protection against anything that might happen as unforeseen. Risk assessment tells us about the factors that might pose a threat to system working , but it doesn’t ensure 100 percent error free systems and the system breakdown , down time, glitches are an equal threat , therefore contingency planning and system testing and evaluation cannot be ruled out despite the best of risk assessments. Risk assessment is the analysis of factors that pose a threat whereas Contingency planning and System evaluation is the practical implementation and step towards ensure the achievement of end product Question # 9: Security testing and Evaluation leads to better security in information technology related products and systems. ST&E positively effects the specifications, development processes, and operational environment. The members related directly to the software packages or hardware and tools are the best ones who can make proper recommendations for the proper working of system. They are the ones who can identify the threats and improvements that can be made in the whole setup. The top management and decision makers are the ones that determine the appropriate action that is being recommended. In other words the middle management is assigned the task of making recommendations and Top management is responsible for deciding for action on suggestions. This is necessary for ensuring the proper functioning and making sure proper measures are taken in time for any mishap that may occur during daily performing of activities in a setup. Question # 10: Risk assessment has to do with the analysis and quantifying of the factors and threats that stand as hurdles in achieving the desired results. System testing and evaluation design team directly contributes to extenuating the risk management and assessment more than the execution team. The execution team is primarily concerned with the practical implementation and contingency planning related activities. The design team provides a platform in form of analyzing all the factors that are risks to the system. Question # 11: Contingency plan requires regular testing and updating because of the need for synchronization with the setup in action. It is being saved that an ounce of prevention is worth a pound of cure. In time Contingency activation can help save time and resources. A fault detected not only consumes time and resources but also eats up the time and resources that would otherwise be used for constructive processes. In other words the backup plan should be a replica of the original setup and all the changes taking place in original setup must be in synch with the backup facility. Question # 12: Contingency plan is performed either part time or in full and this is evident in case of Hot site where the hot site itself serves as contingent option and incase of the enterprise becoming inoperable, all the data and records needed for proper functioning are moved to hot site in itself, other disaster recovery services provide backup options that allows for not acquiring the contingency plan as full time.