Security and mission statement

Chapter: 2 Due date: 20 March 2012 1. What is Mission statement? Why is it important? What does it contain? •Mission statement is a sentence that describes your organization's functions, markets, products/services and advantages. Mission statement elucidates your business, your goals and your objectives. It is used as a constant reminder of why the company exists. •Organizations tend to forget about the purpose of their business after some time. Mission statement is important because it is used as a reminder of why the business exists.

It directs organizations to the initial course of their business as for many companies when the business is growing they tend to get lost and pursue something totally different from their business. •Mission statement reflects every feature of your business. The type of product or service you offer, market position, quality of product or service, customers and more. Eg) Mission for McDonald's is to be their customers' favourite place to be and way to eat. McD exist because of their customers that's why they demonstrate appreciation by providing them with quality and a good service in a clean, welcoming environment at a great value. . What is the primary objective of the secSDLC? What are its major steps, and what are the major objectives of each? •secSDLC is a formal approach to solving problem using a structured sequence of procedures to create inclusive security posture. •Investigation: Management give directions by specifying the goals, processes and the expected outcomes of the project and the costs of the project. At the end of that phase you must have a feasibility study document. •Analysis: The analysis in the secSDLC is when project manager or the team analys the existing security policies, identifying current threats nd attacks

and also Identifying, assessing and evaluating level of risk within the organizations security. •Logical Design: This stage is when security blue print is developed and created and the feasibility study is also developed. •Physical Design: This phase is when the existing physical technology is evaluated and the new physical technology is evaluated also. Alternative solutions are generated and a final design is agreed upon. •Implementation: This stage is when the security solutions are tested and implemented and tested. Personnel issues are evaluated and training is provided.

Security solution are then packaged and sent to management for approval. •Maintenance: After the Information security solutions are implemented they need to be continually tested, monitored and properly managed by means of established procedures. 3. What question may be asked to help identify and classify information assets? Which is the most useful question in the list? •Which information asset is most critical to the success of the organization? •Which information asset generates the most revenue? •Which information asset generates the most profitability? Which information asset would be the most expensive to replace? •Which information asset would be the most expensive to protect? •Which information asset would be most embarrassing or cause the greatest liability if revealed? The most useful question in the list is which information asset is most critical to the success of the organization? This question reflects to the mission statement of the organization. By saying the most " critical asset" to the success of the organization meaning if that asset breaks or it becomes absent the business stops.

Eg) For a retail company say for argument's sake we have the till points, HR department, Accounts, Stalk etc. The till points are the most critical part of

the organization because if the system is down and the tills are not working it means that there is not business for that company for that day until they fix the problem. 4. What term is used to describe the control measure that reduces security incidents amongst member of organization by familiarizing them with relevant policies and practises in an ongoing manner? •SETA Program .