Describe how risk relates to a system security policy.

Security policy defines and documents your organization's established position about the security risks that must be controlled to meet the risk appetite of the business, which will ultimately fund security controls and bear any residual risk.

Describe various risk analysis methodologies.

There are two main types of risk assessment methodologies:

quantitative and qualitative.

A quantitative risk assessment, your organization will start by compiling two lists: a list of possible risks and a list of your most important digital assets. The second list might include items such as valuable information, your IT infrastructure and other key assets. Once you’ve made your list of assets, you’ll assign a dollar value to each item.

A qualitative risk assessment is less about numbers and more about what would actually happen, day-to-day if one of the risks on your list were to occur. While a quantitative risk assessment is straightforward and numbers-based, a qualitative security risk assessment methodology is performed by talking to members of different departments or units and asking them questions about how their operations would be impacted by an attack or a breach.

You joined a small business startup that is in the health services area with no security policy.

Please identify three items that should be included in the policy document for account management that you are asked to develop.

Three Items I would Inclue in the policy are the creation, management and deletion of user accounts; granting and revocation of authorized privileges associated with a user-account; and authentication by which users establish their rights to use a given account. Account management and access control includes the process of requesting, creating, issuing, modifying and disabling user accounts; enabling and disabling access to resources and applications; establishing conditions for group and role membership; tracking accounts and their respective access authorizations.

Would you use a quantitative or qualitative methodology? Explain.

In My organization I would employ a hybrid approach that takes into account quantitative and qualitative inputs.

Risk management is focused on making risk-adjusted decisions to enable your organization to operate efficiently, while taking on as much or as little risk as I deem acceptable.

And the only way to do that is to understand what risks I have, what I am willing to accept and which I wish to transfer, mitigate or avoid.

Account managers maintain accounts. They are the delegated custodians of protected data. Account managers:

* Maintain appropriate levels of communication with the information owners to determine the level or degree of access granted to an individual.
* Determine the technical specifications needed to set access privileges.
* Delegate account management functions to account administrators.
* Create and maintain procedures used in managing accounts.
* Perform all account administrator duties as required.