Public Key Infrastructure

Question 1: The role of the CA in Public Key Infrastructure is to be responsible for issuing and guaranteeing the authentication of certificates. The CA verifies digital signatures on certificates using the public key.

Question 2: In Single Certificate Authority, it is very exposed. If this single certificate authority is compromised, then the entire PKI collapses. In Hierarchical CA, the root is a single point of failure. This means that if the CA is compromised, any leaf or end entities will be a failure and the PKI collapses. To prevent this from happening, the Root is usually offline until certificates are needed and majority of the CA activities are handled by the intermediate CA servers.