Adopting a secure coding standard is very important when it comes to software development. During the design and implementation process, security should always be taken into consideration and not left to the end. This will help increase the layers of defense and decrease chances of vulnerability within the code.

The evaluation and assessment of risk and cost benefit of mitigation is the process where the software development team works with the company to determine which vulnerabilities they should fix based on the risk and cost of the mitigation. The company could even use a priority list to which vulnerability to fix sooner than others based on the potential damage it would be mitigating.

Incorporating zero trust when it comes to security is a great policy to have. It makes sense to have authorization and authentication when it comes to security privileges. This greatly protects assets since it reduces the chance of someone hacking, sabotaging, or negligence.

The implementation and recommendations of security policies makes it so the whole development team is on the same page when it comes to secure coding. The security policies work to protect the software from malicious attacks. The recommendations are based on the evaluation and assessment of risk and cost.