Making sure that you use secure coding standards is important from the beginning to the end of the SDLC. Using best practices and guidelines are important so that you can prevent common vulnerabilities. By doing this from the beginning, you can mitigate security issues and potential breaches. Ensuring adherence to secure coding standards also makes consistency in your coding practices, which makes identifying risks easier.

Risk evaluation and assessment go hand in hand when considering implementing a robust security strategy. There are several steps that go into this which include but are not limited to identifying threats, assessing their impact, and determining how to mitigate them. Cost and benefit is a huge factor when determining the best way to mitigate security risks. By using threat modeling, you can model potential threats and use your results to design effective protections. Once assets and threats are identified, then risks can be organized based on impact.

The zero-trust policy ensures that anyone inside or outside of a network goes through continuous verification. This requires a more granular approach, which means security processes in place must be revamped. Authentication and authorization must be enforced, and constant maintenance must be integrated to mitigate anomalies or potential breaches. This is a policy that cannot support implicit trust, but instead relies on user behavior and device integrity.

Implementation of effective security policies is necessary for making sure the security framework is comprehensive. These policies lay the groundwork for protection from harmful attacks. When looking at it from an organizational perspective, it is crucial to protect their assets and make sure that employees, clients, and developers know how they contribute to maintaining a safe environment.