Secure coding standards are critical to apply to your logical thinking when planning around the design of your software. The concept of not leaving security until the end is a great mindset and principal to code by because it lets you plan around your design the security standards you need to apply. It is the same concept of mapping out your way to work to avoid morning accidents and traffic. If you just got on the road, you may find yourself stuck bumper to bumper, but if you include a plan early to your route, you can find ways to navigate around the issues on the road. If I know I am going to have a lot of user credentials that need authenticated, I will need to plan around the securing this feature from exploits that hackers could exploit in circumventing the authentication.

Evaluating your code for risks is important as this helps identify issues when ran through static analysis tools. It is important to identify all risks early and often to mitigate the risk through the appropriate fixes. This helps eliminate the vulnerability of your software and potential costly issues that could arise if left unchecked. When I identified the risks in the code, I was able to see the severity level and remediation costs as a factor. Mitigating the risk gives a cost benefit as you avoid issues that could generate heavy revenue lost. For example, mitigating a memory buffer that constantly consumes memory if exploited by hackers saves us the chance of a server going down.

Zero trust is a very effective and strict defense strategy model organizations choose to implement with their IT. IT will restrict access controls, access to resources, access to the network and does so without limiting the ability of users on authorized devices from doing their work. It is similar to what I do for people on my home network how only authorized mac addresses can use my network. Even if someone has the password to my Wi-Fi, they would not be able to access the resources of my network without being added to the approved user list. This keeps the organizations environment under a strict access control that lets devices that are authorized to flourish for their end users in all of the needed tasks they are required to accomplish with their job responsibilities.

Implementing security policies based around the assessment of your environment or coding is done after careful planning and use of static analysis tools. Sometimes these policies maybe a series of policies implemented through DevSecOps when basing recommendations around an overhaul of security. This may include how users can be authenticated, network firewalls and work arounds with VPN to ensure a more secure working environment for end users.