***Adoption of a secure coding standard, and not leaving security to the end :***

A secure coding standard I became more familiar with throughout this class would most likely be unit test. During this course we established multiple unit tests and looked into other similar methods like the google tests which come with pretty easy pre-established layouts. As far as not leaving security until the end that was never even an option for me since starting here at SNHU. Being a gamer and techy I always took security seriously, now that I have created and worked on code I have seen how easy it is to cause leaks that could be detrimental. So it should be an ongoing process to constantly make systems more secure.

***Evaluation and assessment of risk and cost benefit of mitigation :***

When it comes to evaluating security risks everything even warnings should be taken into serious. Every exception should be handled as soon as it arises. Also adding redundant layers to help protect sensitive information. The cost benefit of mitigation is massive not just cost wise but also because you can almost never get lost data back truly. Establishing automation for unit testing and updating security is one of the most efficient ways to mitigate errors. The cost benefits of mitigation would be the security net we offer users, if we create a safe application we will generate more consumers.

***Zero trust :***

Zero-trust is a policy I feel that should be incorporated into and application that handles large amounts of sensitive data. We are bursting deeper and deeper into the tech age and we need to create more secure methods to protect individual and their rights, because as it stands now their data could be one click away. So there can be no trust until there are zero harmful attacks or data loss incidents.

***Implementation and recommendations of security policies :***

When it comes to security policies every application and company will have their own needs and wants. The only things that should always be considered is controlling user access for data, user authentication and proper handling when transferring, receiving and storing data. Utilizing automation to update the application and implement new security measures.