**Adoption of a secure coding standard**

Security is a concept that requires effort and planning, just like any other part of the development cycle. Without this effort and planning, security becomes an afterthought that is just added in at the end. Adopting a secure coding standard can help change this. A secure coding standard will help make security a priority throughout the entire development process. Having security be a priority will ensure that it is properly incorporated into the application so that it can be most effective. Incorporating security into the development process will also build good habits for developers so that they code with security in mind.

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

Not all risk is equal, nor will the risks all result in the worst-case scenario. What I mean by this is that some risks will have severe consequences while others may result in nothing more than a minor inconvenience. Each risk that is identified in an organization should be assessed to determine how severe the results would be if the event happened. Once the severity of each risk is determined, we can then assign it a cost. The cost is a value that represents the importance of a risk. A risk with a higher cost is one that should be planned for and mitigated against. A risk with a lower cost is one that should only be mitigated if the mitigations are cost effective and the implementation is easier than if the risk were to actually occur.

**Zero trust**

Zero trust is a concept that is quickly gaining popularity for companies around the world. Zero trust means that there isn’t a single authentication that gives a user access to everything they need, they need to authenticate for each software application that is required for them to complete their jobs. This is becoming popular so quickly due to the increased security it brings. If one login is compromised, that doesn’t mean the malicious actor would be able to gain access to any of the other applications the user can access. If zero trust wasn’t implemented, then the malicious actor would be able to gain access to everything. With the large amounts of data being stored online, it makes more sense having a user authenticate to gain access to each one rather than giving them access to all of it with just a single authentication. Authenticating multiple times is more tedious and time consuming, but it is the overall safer method of accessing private data.

**Implementation and recommendations of security policies**

Implementing a security policy is not an easy task. It takes a lot of planning and time in order for the implementation to go smoothly and be effective. The first step is to determine which standards are the most important and these should be implemented first. Once the entire organization aligns with the standards that are deemed as the most important, then the next set of standards should be implemented. This process should be followed until the entire policy is completely implemented, including current code that is noncompliant and doesn’t meet the standards. The security policy should be reviewed regularly for any shortcomings or updates that need to be done to it. This is my recommendation for how a company should implement a security policy.