Throughout this course we’ve created a security policy that implements the ten core security principles through coding standards and best practices. The coding standards cover topics from SQL injection to proper usage of data types. Best practices include coding examples that adhere to one or more of the core security principles and outlining our policy for authentication, authorization, accounting, and encryption. Our security policy can be summed up by the statement: “Don’t leave security until the end”. That is, when designing or implementing a system security should just as an important component to consider as user experience.

When evaluating risk and weighting it against the cost of mitigation, we referred to the SEI CERT C++ Coding Standard. This standard provides coding standards and risk analysis for them. Risk is determined by a combination of factors such as its severity, likelihood, and remediation cost. Each of these factors need to be considered when determining risk. While one coding standard might have a high likelihood of occurring, it’s severity may be low.

Zero trust is a security framework that requires continuous authentication across users, devices, and applications. The central idea is that no user, device, or application should be implicitly trusted. This security framework is much different from how security used to be viewed. In the past, organizations had their IT systems centralized in one to a few locations. Today, many IT systems are decentralized where a user can navigate between multiple different systems, which create multiple different attack vectors for cyber criminals. Implementing a zero-trust policy makes it much more difficult for an attacker to gain access to and move around your IT system.

As technology evolves at faster rate every year, a continuous review of your security policy is more needed than ever. A security policy should be treated as fluid document. It is a description of how to defend against cyber criminals in the present. As new threats and vulnerabilities are discovered, this document should be updated and new security principles, standards, and best practices should be implemented to combat them.