**Journal: Portfolio Reflection**

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

Adoption of a secure coding standard is important to ensure that you are taking steps towards building secure software. Secure coding standards are a set of guidelines and best practices that are designed to help developers write code that is less vulnerable to security flaws and attacks. This goes along with not leaving security until the end, security should be a priority throughout the entire software development process. Security considerations should be integrated into every stage of the software development lifecycle.

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

Evaluation and assessment of risk and cost benefit of mitigation involves identifying potential security risks and vulnerabilities, accessing the likelihood and potential impact of the risks, and determining the cost and benefits of implementing mitigation measures to address the risk. By evaluating and assessing the risk and cost-benefit of mitigation measures, organizations can develop a more effective security strategy that balances the need to protect against potential security risks with the need to manage costs and resources.

* **Zero trust**

Zero trust is a security model that assumes that all devices, applications, and users are potentially compromised and should not be trusted by default. Under the zero-trust model, access to resources and systems is granted on a need-to-know basis, with strict controls in place to limit access to sensitive data and functionality. By adopting the zero trust model organizations can better protect their sensitive data and systems, reduce the risk of security breaches, and improve their overall security.

**Implementation and recommendations of security policies**

The steps of implementing an effective security policy are to identify your security goals. Start by identifying your organization's security goals and what you want to achieve with your security policies. Next, you will develop a comprehensive security policy framework that covers all areas of the organization’s security posture. For your security policy to be effective you will need to keep the policies up to date, communicate policies make sure everyone in the organization understands and works towards the security policy, and monitor compliance. You must ensure that all employees are following the security policy.