Portfolio Reflection

* Adoption of a Secure Coding Standard:
  + Importance: Adopting a secure coding standard is crucial as it sets the foundation for writing secure software from the beginning. It helps developers understand best practices, reduces vulnerabilities, and improves overall code quality.
  + Supporting Readings: References like "Secure Coding Guidelines" by CERT/CC and "The CERT C Coding Standard" provide comprehensive guidelines for writing secure code in C and other languages. These standards cover topics such as input validation, memory management, and handling sensitive data securely.
* Evaluation and Assessment of Risk and Cost-Benefit of Mitigation:
  + Risk Assessment: Understanding the risks associated with potential vulnerabilities is essential. This involves identifying threats, assessing their impact and likelihood, and prioritizing mitigation efforts based on risk severity.
  + Cost-Benefit Analysis: Evaluating the cost of implementing security measures against the potential cost of a security breach is crucial. This analysis helps in making informed decisions about where to allocate resources for maximum risk reduction.
  + Supporting Readings: "Security Risk Assessment and Management: A Detailed Overview" provides methodologies for conducting risk assessments. "Cost-Benefit Analysis of Security Measures" discusses approaches to evaluating the cost-effectiveness of security solutions.
* Zero Trust:
  + Concept: Zero trust is a security model based on the principle of "never trust, always verify." It assumes that threats can exist both inside and outside the network, and access controls should be continuously verified.
  + Implementation: Implementing zero trust involves strong authentication, continuous monitoring, and strict access controls based on least privilege.
  + Supporting Readings: "Zero Trust Architecture" by NIST and "The Forrester Wave™: Zero Trust eXtended Ecosystem Platform Providers, Q3 2021" offer insights into zero trust principles and implementation strategies.
* Implementation and Recommendations of Security Policies:
  + Policy Implementation: Security policies define rules and guidelines for protecting assets, such as data, systems, and networks. Implementing these policies involves both technical measures (e.g., access controls, encryption) and organizational practices (e.g., training, incident response).
  + Recommendations: Best practices for security policies include regular updates, employee training, incident response plans, and compliance with relevant standards and regulations.
  + Supporting Readings: "Information Security Policy: Definition and Best Practices" outlines the components of an effective security policy. "ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems -- Requirements" provides a framework for implementing an information security management system.