**Reflection**

Adopting a secure coding standard is essential in ensuring that security is integrated throughout the software development lifecycle (SDLC) rather than being an afterthought. Secure coding standards provide guidelines and best practices that developers must follow to prevent common vulnerabilities such as SQL injection, cross-site scripting (XSS), and buffer overflows. By adhering to these standards from the beginning, developers can mitigate risks early, reducing the likelihood of security breaches.

Evaluating and assessing risk is crucial in prioritizing security efforts and allocating resources effectively. This involves identifying potential threats, assessing their likelihood and impact, and determining the cost-benefit of various mitigation strategies. A practical approach to this is the use of frameworks such as STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) and DREAD (Damage, Reproducibility, Exploitability, Affected Users, Discoverability), which help in systematically assessing risks and deciding on appropriate mitigation measures.

The "Risk Management Framework" by NIST provides a comprehensive methodology for evaluating risks and implementing cost-effective controls. The framework emphasizes continuous monitoring and assessment, ensuring that risk management is an ongoing process. By evaluating the cost and benefits of different mitigation strategies, organizations can implement security measures that provide the most value in reducing risks.

**Zero Trust:**

The Zero Trust security model operates on the principle that no entity, whether inside or outside the network, should be trusted by default. Instead, every access request is verified, and least privilege access is enforced. This approach significantly reduces the attack surface and limits the potential impact of a security breach.

The concept of Zero Trust is well-articulated in the paper "BeyondCorp: A New Approach to Enterprise Security" by Google. It highlights the need for continuous authentication and authorization, leveraging strong identity verification and access controls. Implementing a Zero Trust model requires a shift in mindset and architecture, focusing on securing data and resources rather than just the perimeter.

**Implementation and Recommendations of Security Policies:**

Implementing effective security policies is critical in establishing a secure environment. Security policies provide a framework for managing and protecting sensitive information, defining roles and responsibilities, and setting procedures for incident response. These policies should be clear, enforceable, and regularly updated to reflect evolving threats and technologies.

The "ISO/IEC 27001:2013 Information Security Management" standard provides guidelines for developing and implementing security policies. It emphasizes the importance of a risk-based approach, continuous improvement, and top management commitment. Recommendations for security policies include defining acceptable use, access control, incident response, and employee training. Regular audits and reviews ensure that policies remain effective and relevant.