The adoption of a secure coding standard emphasizes the importance of incorporating security measures from the start of software development, rather than leaving it until the end. This approach aims to proactively address potential vulnerabilities and minimize security risks throughout the development process.

Evaluating risks and analyzing the cost benefit of mitigation considers factors such as the likelihood of an attack, the impact on the system or organization, and the cost-effectiveness of implementing security measures.

Zero trust is a security model based on the principle of never automatically trusting any entity, both inside and outside the network. Instead, it requires strict verification of all users, devices, and applications attempting to access resources, regardless of their location (Zscaler, 2024).

Implementation and recommendations of security policies involve establishing guidelines and protocols to protect an organization's assets and data. This includes defining access controls, encryption methods, and authentication procedures to ensure that only authorized users can access sensitive information (Grimmick, 2023).

**References**

Grimmick, R. (2023). What is a security policy? Definition, Elements, and Examples. Retrieved April 22, 2024 from <https://www.varonis.com/blog/what-is-a-security-policy#Four_reasons_a_security_policy_is_important>

Zscaler. (2024). What is zero trust? Retrieved April 23, 2024 from <https://www.zscaler.com/resources/security-terms-glossary/what-is-zero-trust>