



Security Practices Journal

Security is not something that can be added to software after the fact. Adopting a secure coding standard from the very beginning of a project is essential to building reliable and trustworthy systems. Secure coding means writing software in a way that protects it from vulnerabilities and attacks (Veracode, 2023). When developers follow established standards, they reduce the chance of introducing flaws that attackers can exploit. Security issues are far more costly to fix after deployment than during development (OWASP, 2023). Waiting until the end of a project to address security is a risky and expensive approach. Security must be treated as a core requirement from the start, not an afterthought.

Integrating security into the software development lifecycle also makes financial sense. Fixing security defects early in the agile process is significantly cheaper than addressing them in later phases (Ouedraogo et al., 2022). When a team identifies a vulnerability during the design phase, the cost to fix it is minimal compared to fixing it after the product has shipped. A cost-benefit analysis helps organizations decide which security controls to implement based on the potential losses they prevent versus the resources required. Organizations should evaluate each risk by estimating its likelihood and potential impact (Fruhlinger, 2021). This process allows teams to prioritize security investments wisely. Not every threat requires the same level of response, and understanding the trade-offs helps teams make better decisions.

Zero trust is a security model that operates on the principle of never automatically trusting any user, device, or system. Zero trust requires continuous verification of every entity



that attempts to access resources (CISA, 2021). This approach is especially important in modern environments where remote work and cloud services have expanded the attack surface.

Traditional perimeter-based security assumes that users inside the network are safe, but zero trust rejects that assumption. Instead, access is granted based on verified identity, device health, and the principle of least privilege. Organizations should implement zero trust in stages, beginning with identifying critical assets and mapping data flows (Palo Alto Networks, 2022). Security policies should reflect the zero trust model by requiring multi-factor authentication, enforcing strict access controls, and monitoring all network traffic continuously. Written policies provide the foundation for consistent security practices across an organization (SANS Institute, 2023).

Without clear policies, individuals may make inconsistent decisions that introduce risk.

Combining zero trust principles with strong, well-documented security policies gives organizations a practical and resilient security posture.

Taking a proactive approach to security means addressing it at every stage of development and operations. Secure coding standards prevent vulnerabilities before they can be exploited (Veracode, 2023; OWASP, 2023). Cost-benefit analysis ensures that security spending is targeted and justified (Fruhlinger, 2021; Ouedraogo et al., 2022). Zero trust policies reduce the risk of unauthorized access in complex and distributed environments (CISA, 2021; Palo Alto Networks, 2022). Together, these practices form a comprehensive strategy for managing security risk. Organizations that adopt these principles are better prepared to protect their data, their users, and their reputation.

References

CISA. (2021). *Understanding the zero trust security model to safeguard digital infrastructure.* Cybersecurity and Infrastructure Security Agency. <https://www.cisa.gov/zero-trust-maturity-model>

Fruhlinger, J. (2021). *Cost benefit analysis in security: How to use cost benefit analysis to balance the security risks and costs.* CSO Online.
<https://www.csoonline.com/article/cost-benefit-analysis-security.html>

OWASP. (2023). *Secure coding: A practical guide.* Open Worldwide Application Security Project. <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/>

Ouedraogo, M., Mouratidis, H., Preston, D., & Khadraoui, D. (2022). *Cost benefit analysis of incorporating security and evaluation of its effects on various phases of agile software development.* Journal of Information Security and Applications, 65, 103102.
<https://doi.org/10.1016/j.jisa.2022.103102>

Palo Alto Networks. (2022). *A practical guide to zero-trust security.*
<https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture>

SANS Institute. (2023). *Information security policies: Why they are important to your organization.* <https://www.sans.org/white-papers/information-security-policies-important-organization/>

Veracode. (2023). *What is secure coding and why is it important?*
<https://www.veracode.com/security/secure-coding>