* Adoption of a Secure Coding Standard and Not Leaving Security to the End
  + Organizations increasingly recognize the importance of initially integrating secure coding standards into their software development processes rather than treating security as an afterthought. This involves adopting best practices and guidelines for writing secure code to mitigate vulnerabilities and enhance overall system security.
* Evaluation and Assessment of Risk and Cost Benefit of Mitigation
  + Risk assessment and cost mitigation evaluation involve systematically analyzing potential risks to an organization's assets, operations, and reputation and calculating the costs and benefits of implementing various mitigation measures. It aims to inform decision-making by comprehensively understanding the risks and the value of different risk mitigation strategies.
* Zero Trust:
  + Zero Trust is a security concept centered around the notion that organizations should not automatically trust anything inside or outside their perimeters and must verify everything trying to connect to its systems before granting access. This approach assumes that breaches are inevitable and focuses on strict access controls and continuous monitoring to minimize the potential damage.
* Implementation and Recommendations of Security Policies:
  + Implementing these security policies involves establishing specific rules, procedures, and technical measures to safeguard an organization's information assets. Effective security policies outline guidelines for data protection, access control, incident response, and other aspects of cybersecurity, providing a framework for secure operations and risk management.

The evolving landscape of cybersecurity demands a proactive approach to secure software development, with organizations increasingly prioritizing adopting secure coding standards and integrating security from the outset of the development process. Concurrently, the evaluation and assessment of risk and the cost-benefit of mitigation strategies play a crucial role in informing informed decision-making. Embracing the Zero Trust model has become pivotal, emphasizing stringent access controls and continuous monitoring to mitigate potential damage. Furthermore, implementing and adhering to robust security policies are essential, providing a framework for safeguarding information assets and guiding secure operations and risk management. These interconnected elements collectively contribute to a comprehensive and proactive approach to cybersecurity.