* Adoption of a secure coding standard, and not leaving security to the end  
    
   Insuring that a secure coding standard is being used is a very important practice to follow. This will set guidelines for every person on a team to help keep everyone on the same page. A coding standard can also include the practice of not leaving security to the end which is the idea of making sure security is thought about through the entire SDLC. This practice can help catch security issues early on instead of just during final testing. There is a good chance that if these issues are left to the end that a domino effect of issues can occur rather than the single issue that it was because all the code after the issue was built on the old problem code.
* Evaluation and assessment of risk and cost benefit of mitigation  
    
   This is a concept that is asking if the risk of the potential threat is worth the cost to protect from this risk. This can be like a pro con list where you are trying to determine if the amount of good and potential threats you can eliminate are valued higher then the data that could potentially be accessed and the cost required to implement a fix
* Zero trust  
    
   This is making the default setting for all users have no access to any kind of data. This “never trust, always verify” method ensures that at every step of the way anyone that is inside a system is being checked and verified that they are supposed to be where they are at in the system. This can mean that there is a bit more of a cost to the system but like the last topic talks about the reward for using this level of security can be valued more than this cost.
* Implementation and recommendations of security policies  
    
   Similar to the coding standards this is a great way to make sure there is a base set of guidelines to follow, especially in a team where everyone needs to be on the same page. This can make sure everyone is aware of the requirements involved and give procedures to follow for a large range of issues that may come up.