Some examples of adopting a secure coding standard and not leaving security to the end:

1. Making sure platforms and programming languages such as C++, Python, Javascript are secure.
2. **Proper Input Validation** is vital on the Command Line, Network Interfaces, etc. to so we don’t provide invalid data, or data that results in errors because that would open up vulnerabilities
3. **Implicit deny** by default so traffic doesn’t flow in and out from anywhere.
4. Utilizing the highest warning level on a compiler to compile our code. This allows us to modify the program to where we lessen errors.
5. **Defense in Depth** is a method where we implement layers of defense for multiple points of security.
6. **Error Handling And Logging** to catch those errors that show up in our system and to audit those errors so we know what to fix.

**Risk Evaluation** is defining how severe a risk is in correspondence with other risks. **Risk Assessment** is recognizing hazards and assessing any correlating risks in the organization. After this step is done, action is executed to either mitigate or remove these threats. **Cost -Benefit Of Mitigation** allows organizations to produce more profit, increase pay of labor workers, allow consumers to buy products at a cheaper rate.

**Zero Trust** is a security concept in which the organization doesn’t trust anyone or anything whether the factors are internal or external. They verify intentions before giving access to their system.

Implementation of security policies are identifying risks present to make sure the policy is updated to take care of that risk. User training is important as well because we can have all of these technical and administrative controls in place but if a user is ignorant and unaware of his actions and surroundings, it makes it that much easier for malicious activity to find its way into an organization. Installation of proper tools such as Anti-Viruses are important as well too so we are better equipped in setting up our security and defenses.

Recommendations of security policies are strong passwords that meet complexity requirements so attacks such as brute force, dictionary, password spraying are ineffective. Secure Wi-fi so attackers have a harder time accessing personal files and data. Backups are important to to make sure data can be accessed at all times