Adoption of a secure coding standard, and not leaving security to the end

Adoption of a secure coding standard helps understand the risks, threat levels, and principles that align with each standard. For instance, coding standard data type will ensure that signed integers do not overflow/underflow. The principles, for this standard, are to validate user input, heed compiler warnings, and use effective quality assurance techniques. These principles will ensure input data is tested, alert with warnings, and validated. This will avoid leaving security to the end. It is best to implement security throughout the whole development process to find and fix issues and increase security measures in the beginning to the end of the process.

Evaluation and assessment of risk and cost benefit of mitigation.

Having evaluation and assessment of risks and cost, this will tell what the company is up against if the system was compromised. It is best to have this in place in a policy to understand the likelihood of what ifs later down the road. This will also detail what needs to be addressed before the system is compromised.

Zero trust

Zero trust should be used by ever developer to ensure everyone’s information is safe across the board, inside or outside of the network. Zero trust incorporates multifaceted security levels such as verify, identification, authorization, and accounts. It is used in combination with the Triple A policy or vice versa. The level of security depends on the users, privileges, and authorizations. Accounting comes in to play by logging the system by keeping track of who is on the network and what is being always done to/on the network.

Implementation and recommendations of security policies

For the safest, securest systems, all security policies should be incorporated. The Triple A policy was mentioned about and should be implemented as well as zero trust, risks and the adoption of coding standards and principles. Most systems will differ as far as needs of security but no one system should be unsecure and extra measures should be incorporated as well as defense in depth.