Not leaving security to the end is another way of saying how important it is to always prioritize security. This is the forefront of development and should always be considered the best practice to create with the most security in mind. When security is not left for after there is more likely that there are more vulnerabilities and on the other hand when security is thought of first you can build your code around the necessary security requirements. This is the first step that always needs to be taken to ensure best practice.

When looking at the assessment of risk this is when you can take a look back at your code and determine what might require more security. This is a way for the developer to take a deeper look at the code and realize what needs to be the most secure to fulfill your ethical duty. It is also important to look into how the cost benefits before making major changes. This is because some security measures may be considered overboard and if the threat level is too extreme then it may still be beneficial to spend more time and resources to secure it.

Zero Trust is a method that is similar to the idea of putting security at the forefront of development. This is because it is a way to start and stay throughout the program’s life span to protect against the possible user threats. This is the idea that when you give some trust to users there will always be someone that abuses that trust. It is always best practice to create software with the most security as possible to protect client and user data. In this method especially it is used to protect clients by allowing them to see and limit user activity.

Overall, it is always important to follow and learn best practice for building a secure project. You can also learn your company security policies and make sure that they are being enforced by you and your team. It is also important to set an example by following these policies and informing and encouraging your team members to also follow these policies.