* Adoption of a secure coding standard, and not leaving security to the end
  + The adoption of the specific coding standard idea of Defense in Depth is what allows for the continuous support of software and data. Alongside this, we also used SEI CERT standards to help build project 1 and project 2 Green Pace security standards.
* Evaluation and assessment of risk and cost benefit of mitigation
  + Evaluating and assessing the risk/cost benefit of mitigation is what helps to get new security policies understood and implemented. This is what lays out the benefits and potential drawbacks of mitigation. To reference the project 1 security standards, this assessment typically comprises of severity, likelihood, remediation cost, and priority.
* Zero trust
  + The zero-trust standard means to verify the users constantly and use the principle of least privilege to prevent and mitigate potential security attacks from both outside users and inside users.
* Implementation and recommendations of security policies
  + The implementation and recommendations of security policies and procedures, such as defense in depth and zero trust, is what integrates security into the DevOps life cycle. This, in turn, creates DevSecOps with continuous security throughout the software development life cycle.