The words policy, standard, procedure and guideline relate to each other as they help shape how security rules are written and enforced. A policy is used to set ideas or intended plans, for example being how a penetration test must be authorized and controlled. A standard gives specific requirements and regulations, like how long testing should occur and what information should be deemed necessary for the experiment. Procedure describes the step by step method that is taken for those testing to fall back upon during the engagement. And finally, a guideline offers the best practices and recommendations to support consistency, a much looser term compared to something like rules which deem what one can or can't do. All four of these words together in practice create a balance between being flexible and accountable. Owners and approvers set the groundwork for each layer of this hierarchy, whereas a review cadence maintains the policies are up to date and effective. Enforcement ensures accountability and principles which are aligned in the Ebook and policies such as ISO/IEC 27001's Information security policy.

In a rules of engagement, a document that is required in the cybersecurity field for penetrating testing, there are several clauses that are detailed and highlight the importance of what the authorized person can do during testing. However, the ones that I view are the most essential in the document happen to be scope and data handling. Scope sets the standards that are required for the person doing the penetration testing. Actions and tools that can be used during the experiment while also limiting or prohibiting actions that cannot be done during the time. Data handling is essential as it dictates what needs to be done and what has happened with the gathered necessary sensitive information obtained from the testing. By only collecting the necessary minimum data, we can reduce the risk of mishandling sensitive information and preserve the trust of the authorizers. These two clauses in a rules of engagement document are necessary as they uphold security while also maintaining consistency and showing legal obligations.

One area that I find that has remained unclear is how authorization is validated across shared or third party systems. If a test involves a cloud infrastructure, does the approval automatically extend to that infrastructure or is there a secondary authorization needed to search in that area? A question I feel that should be asked as it plays into the legality and safety of the operations engagement.

In the portfolio, I will be including:

- My document on the Rules of Engagement or how one would be filled out/
- My weekly reflection which reveal not only which portions of the RoE document are the most necessary and how the words policy, standard, procedure and guideline relate to each other.