We follow the industry standard OWASP procedural Checklist. Checklist is attached.The flow diagram below is based around several steps:

- The penetration test starts by gathering all possible information available regarding the infrastructure and applications involved. This stage is paramount as without a solid understanding of the underlying technology involved, sections may be missed during the testing phase

- The test should follow all the different phases described below

- Testers should attempt to exploit all discovered vulnerabilities. Even if the exploitation fails, the tester will have a better understanding of the vulnerability risk

- Any information returned by checking for vulnerabilities, for example, programming errors, source code retrieval or other internal information disclosure, should be used to re-assess the overall understanding of the application and how it performs

- If at any point during the testing a vulnerability is detected, which may lead to the successful compromise of the target or disclose business-critical information, the relevant contact for the company should be contacted immediately and made aware of the situation and risks involved.

A close up of a logo

Description automatically generated