**Goal & Scope Identification**

**Goal**

* Identify the outcome
* Identify sub-goals
* Any extra services that were asked to be tested
* 1-2 sentences long

**Scope**

* What is the range of assessments
* What is off-limits
* What are the restrictions of the assessment
* Can be anything from a single service or host to an entire network segment

**Stability considerations**

* Need to know if a service, network, etc is fragile
  + If a firewall is running to high or an uplink at capacity etc.
    - A simple port scan through a fragile uplink could bring down an entire network segment
* Owners of the services, networks etc. may know about the stability issues

**What should we look out for**

* Sensitive services
* Exploits with memory corruption
* Attacker traffic on network devices, excluding port scans
* Unstable exploits
* Non-HA systems
  + High availability

**Paper Trail**

* Keep track of emails, communications, documents, etc that have approval of these considerations, goal and scope restrictions