Question 1:

Review section 1.5.2 (a-i) Conducting the Pen Test.

What is the focus and intent of these steps?

The focus and intent of these steps are simply to oversee the penetration test as well as appointing someone to be the Point of Contact (POC). This POC will be in charge of managing the penetration test as well as notifying the managers and higher-ups of the planned testing.

They will also be in charge of documentation as well as the original plans for the Pen Test. They get to make a team and appoint roles as they deem necessary.

What seems to be the priorities?

The priorities seem to be focused around keeping the project contained and managed efficiently. Keeping it contained within the given guidelines, as well as alerting the management of the plans as well as the schedules. The POC is the leader of the team who is able to assign workers where necessary in order to make sure the whole test goes according to plan.

Question 2:

Review Appendix A. - Penetration Test Plan

How does this Plan relate to the Attack Methodology we covered in class?

The Plans of "Attack" covered in class were very similar to the list created in the NASA SOP.

In-Class	NASA SOP
1. Reconnaissance 2. Scanning 3. Exploitation 4. Post-Exploitation & Maintaining Access 5. Reporting	1. Planning and Enumeration a. This is where the Scope is identified as well as the Rules of Engagement. b. Report vulnerabilities as well as any other findings and present them to the on-site admins to test these. 2. Vulnerability Analysis

	a. Identifying targets, vulnerabilities, performing tests, etc. 3. Penetration Testing a. Executing attacks as well as recording results. Report and analyze findings and begin trying to solve these issues.
While NASA's list is less steps, it is much more concise within each step. Each step is also to be used as a guideline for the report that is necessary for the write up after the test is complete.	

How does it correspond to the Course Syllabus?

It forces the people performing the pen test to sign off on their work saying that it is strictly for reporting and solving their issues, with very little wiggle room for error.

Question 3:

Review Appendix B. Rules to be Followed

Identify 2 rules that may limit the testers from fully identifying all potential vulnerabilities.

"Prior to any war dialing efforts, a 'Do Not Call' list will be provided to the [Third party}

Penetration team. The team shall configure their environment to strictly adhere to this

'Do Not Call' list"

This list can cause a possible vulnerability that would have been spotted in a war dialing to not be noticed.

"A full network scan will not be performed. A targeted network scan will be completed

and limited to the subnets and targeted hosts, so as to control and further minimize load

on the network infrastructure."

While this rule should be in place, obviously a targeted scan will not return as much information as a large-scale scan of the whole network. The rule also states the attacker will refrain from any DOS attacks.

Question 4: Optional

What is War Dialing?

War Dialing is a form of testing where a list of many phone numbers are read and dialed, often in order to find any weak points in the business being tested. This is used to locate unprotected modems which can be potentially exploited in the future.

Source: https://www.techopedia.com/definition/15505/wardialing