Remember that a security audit verifies compliance and a security assessment validates vulnerabilities. An organization should employ both to capture complete perspective of the overall security stance. A company should know where violations happen or vulnerabilities exist in their own networks. Auditing system policies and assessing system security require the following certain procedures in a specific order.

The following procedures are out of order. Sort them in the order of priority.

**Hint:** Consider how each step is dependent on the one before it.

**Auditing system policies:**

1. Establish audit benchmarks and baselines. \_\_\_\_\_\_\_\_
2. Verify accuracy of controls and compliant operation. \_\_\_\_\_\_\_\_
3. Define the audit plan. \_\_\_\_\_\_\_\_
4. Collect audit data and conduct interviews. \_\_\_\_\_\_\_\_
5. Identify in-scope and out-of-scope objectives. \_\_\_\_\_\_\_\_
6. Select and review policies, procedures, and planning documents. \_\_\_\_\_\_\_\_

**Assessing system security:**

1. Identify in-scope and out-of-scope objectives. \_\_\_\_\_\_\_\_
2. Validate security mechanisms and identify true weaknesses. \_\_\_\_\_\_\_\_
3. Define the assessment plan. \_\_\_\_\_\_\_\_
4. Collect assessment data and conduct interviews. \_\_\_\_\_\_\_\_
5. Establish assessment benchmarks and baselines. \_\_\_\_\_\_\_\_
6. Target applications, connections, protocols, services, or users to exploit. \_\_\_\_\_\_\_\_