OSSTMM

The Open Source Security Testing Methodology Manual provides a detailed framework of testing strategies for systems, software, applications, communications and the human aspect of cybersecurity.

The methodology focuses primarily on how these systems, applications communicate, so it includes a methodology for:

1. **Telecommunications (phones, VoIP, etc.)**
2. Wired Networks
3. Wireless communications

Advantages	Disadvantages
Covers various testing strategies in-depth.	The framework is difficult to understand, very detailed, and tends to use unique definitions.
Includes testing strategies for specific targets (I.e. telecommunications and networking)	*Intentionally left blank.*
The framework is flexible depending upon the organisation's needs.	*Intentionally left blank.*
The framework is meant to set a standard for systems and applications, meaning that a universal methodology can be used in a penetration testing scenario.	*Intentionally left blank.*

Revision #2
Created 2023-02-11 20:36:20 UTC by Fettlaus
Updated 2023-02-11 20:46:44 UTC by Fettlaus