

**Fact does not come from the grand leaps of discovery but rather from the small, careful steps of verification.**



# Chapter 2 – What You Need to Do

Where do you start? Testing is a complicated affair and with anything complicated, you approach it in small, comprehensible pieces to be sure you don't make mistakes.

Conventional wisdom says complexity is an enemy of security. However, it is only at odds with human nature. Anything which is made more complex is not inherently insecure. Consider a computer managing complex tasks. The problem as we know it is not that the computer will make mistakes, confuse the tasks, or forget to complete some. As more tasks are added to the computer, it gets slower and slower, taking more time to complete all the tasks. People, however, do make mistakes, forget tasks, and purposely abandon tasks which are either not important or required at the moment. So when testing security, what you need to do is properly manage any complexity. This is done by properly defining the security test.

## 2.1 Defining a Security Test

These 7 steps will take you to the start of a properly defined security test.

1. Define what you want to protect. These are the assets. The protection mechanisms for these assets are the **Controls** you will test to identify **Limitations**.
2. Identify the area around the assets which includes the protection mechanisms and the processes or services built around the assets. This is where interaction with assets will take place. This is your **engagement zone**.
3. Define everything outside the engagement zone that you need to keep your assets operational. This may include things you may not be able to directly influence like electricity, food, water, air, stable ground, information, legislation, regulations and things you may be able to work with like dryness, warmth, coolness, clarity, contractors, colleagues, branding, partnerships, and so on. Also count that which keeps the infrastructure operational like processes, protocols, and continued resources. This is your test **scope**.
4. Define how your scope interacts within itself and with the outside. Logically compartmentalize the assets within the scope through the direction of interactions such as inside to outside, outside to inside, inside to inside, department A to department B, etc. These are your **vectors**. Each vector should ideally be a separate test to keep each compartmentalized test duration short before too much change can occur within the environment.
5. Identify what equipment will be needed for each test. Inside each vector, interactions may occur on various levels. These levels may be classified in many ways, however here they have been classified by function as five **channels**. The channels are Human, Physical, Wireless, Telecommunications, and Data Networks. Each channel must be separately tested for each vector.
6. Determine what information you want to learn from the test. Will you be testing interactions with the assets or also the response from active security measures? The **test type** must be individually defined for each test, however there are six common types identified here as Blind, Double Blind, Gray Box, Double Gray Box, Tandem, and Reversal.
7. Assure the security test you have defined is in compliance to the **Rules of Engagement**, a guideline to assure the process for a proper security test without creating misunderstandings, misconceptions, or false expectations.

The end result will be a measurement of your **Attack Surface**. The attack surface is the unprotected part of the Scope from a defined Vector.



### 2.2 Scope

The scope is the total possible operating security environment for any interaction with any asset which may include the physical components of security measures as well. The scope is comprised of three classes of which there are five channels: Telecommunications and Data Networks security Channels of the COMMSEC class, Physical and Human Security Channels of the PHYSSEC class, and the full spectrum Wireless Security Channel of the SPECSEC class. Classes are from official designations currently in use in the security industry, government, and the military. Classes are used to define an area of study, investigation, or operation. However, Channels are the specific means of interacting with assets. An asset can be anything that has value to the owner. Assets can be physical property like gold, people, blueprints, laptops, the typical 900 MHz frequency phone signal, and money; or intellectual property such as personnel data, a relationship, a brand, business processes, passwords, and something which is said over the 900 MHz phone signal. Often, the scope extends far beyond the reach of the asset owner as dependencies are beyond the asset owner's ability to provide independently. The scope requires that all threats be considered possible, even if not probable. Although, it must be made clear that a security analysis must be restricted to that which is within a type of certainty (not to be confused with risk which is not a certainty but a probability). These restrictions include:

1. Non-events such as a volcano eruption where no volcano exists,
2. Non-impact like moonlight through data center window, or
3. Global-impacting such as a catastrophic meteor impact.

While a thorough security audit requires testing all five channels, realistically, tests are conducted and categorized by the required expertise of the Analyst and the required equipment for the audit.



## Channels

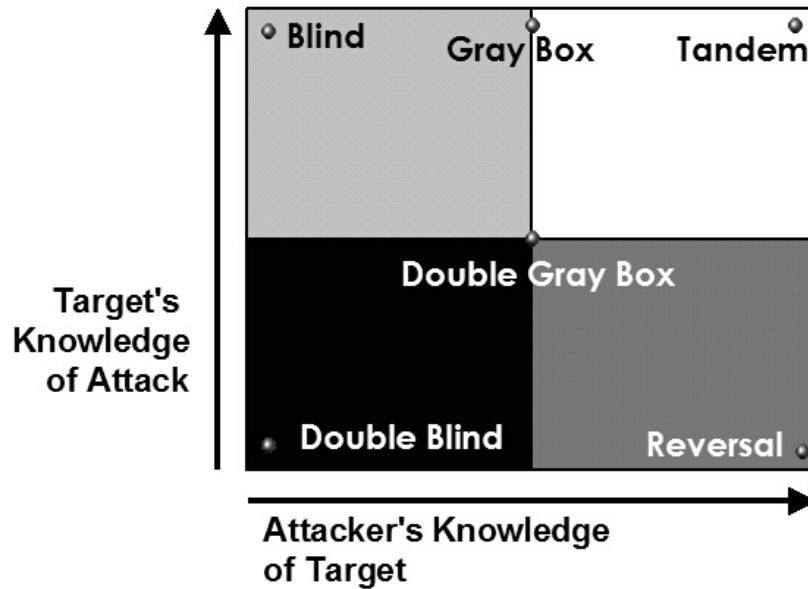
Class	Channel	Description
Physical Security (PHYSSEC)	Human	Comprises the human element of communication where interaction is either physical or psychological.
	Physical	Physical security testing where the channel is both physical and non-electronic in nature. Comprises the tangible element of security where interaction requires physical effort or an energy transmitter to manipulate.
Spectrum Security (SPECSEC)	Wireless	Comprises all electronic communications, signals, and emanations which take place over the known EM spectrum. This includes ELSEC as electronic communications, SIGSEC as signals, and EMSEC which are emanations untethered by cables.
Communications Security (COMMSEC)	Telecommunications	Comprises all telecommunication networks, digital or analog, where interaction takes place over established telephone or telephone-like network lines.
	Data Networks	Comprises all electronic systems and data networks where interaction takes place over established cable and wired network lines. Data Networks

While the channels and their divisions may be represented in any way, within this manual they are organized as recognizable means of communication and interaction. This organization is designed to facilitate the test process while minimizing the inefficient overhead that is often associated with strict methodologies.



## 2.3 Common Test Types

These six types differ based on the amount of information the tester knows about the targets, what the target knows about the tester or expects from the test, and the legitimacy of the test. Some tests will test the tester's skill more than actually testing the security of a target.



Do note when reporting the audit, there is often a requirement to identify exactly the type of audit performed. Too often, audits based on different test types are compared to track the delta (deviations) from an established baseline of the scope. If the precise test type is not available to a third-party reviewer or regulator, the audit itself should be considered a Blind test, which is one with the least merit towards a thorough security test.



## OSSTMM 3 – The Open Source Security Testing Methodology Manual

Type		Description
1	Blind	The Analyst engages the target with no prior knowledge of its defenses, assets, or channels. The target is prepared for the audit, knowing in advance all the details of the audit. A blind audit primarily tests the skills of the Analyst. The breadth and depth of a blind audit can only be as vast as the Analyst's applicable knowledge and efficiency allows. In COMMSEC and SPECSEC, this is often referred to as Ethical Hacking and in the PHYSSEC class, this is generally scripted as <b>War Gaming</b> or <b>Role Playing</b> .
2	Double Blind	The Analyst engages the target with no prior knowledge of its defenses, assets, or channels. The target is not notified in advance of the scope of the audit, the channels tested, or the test vectors. A double blind audit tests the skills of the Analyst and the preparedness of the target to unknown variables of agitation. The breadth and depth of any blind audit can only be as vast as the Analyst's applicable knowledge and efficiency allows. This is also known as a <b>Black Box test</b> or <b>Penetration test</b> .
3	Gray Box	The Analyst engages the target with limited knowledge of its defenses and assets and full knowledge of channels. The target is prepared for the audit, knowing in advance all the details of the audit. A gray box audit tests the skills of the Analyst. The nature of the test is efficiency. The breadth and depth depends upon the quality of the information provided to the Analyst before the test as well as the Analyst's applicable knowledge. This type of test is often referred to as a <b>Vulnerability Test</b> and is most often initiated by the target as a self-assessment.
4	Double Gray Box	The Analyst engages the target with limited knowledge of its defenses and assets and full knowledge of channels. The target is notified in advance of the scope and time frame of the audit but not the channels tested or the test vectors. A double gray box audit tests the skills of the Analyst and the target's preparedness to unknown variables of agitation. The breadth and depth depends upon the quality of the information provided to the Analyst and the target before the test as well as the Analyst's applicable knowledge. This is also known as a <b>White Box test</b> .
5	Tandem	The Analyst and the target are prepared for the audit, both knowing in advance all the details of the audit. A tandem audit tests the protection and controls of the target. However, it cannot test the preparedness of the target to unknown variables of agitation. The true nature of the test is thoroughness as the Analyst does have full view of all tests and their responses. The breadth and depth depends upon the quality of the information provided to the Analyst before the test (transparency) as well as the Analyst's applicable knowledge. This is often known as an In-House Audit or a <b>Crystal Box test</b> and the Analyst is often part of the security process.
6	Reversal	The Analyst engages the target with full knowledge of its processes and operational security, but the target knows nothing of what, how, or when the Analyst will be testing. The true nature of this test is to audit the preparedness of the target to unknown variables and vectors of agitation. The breadth and depth depends upon the quality of the information provided to the Analyst and the Analyst's applicable knowledge and creativity. This is also often called a <b>Red Team exercise</b> .



### 2.4 Rules Of Engagement

These rules define the operational guidelines of acceptable practices in marketing and selling testing, performing testing work, and handling the results of testing engagements.

#### A. Sales and Marketing

1. The use of fear, uncertainty, doubt, and deception may not be used in the sales or marketing presentations, websites, supporting materials, reports, or discussion of security testing for the purpose of selling or providing security tests. This includes but is not limited to highlighting crimes, facts, glorified criminal or hacker profiles, and statistics to motivate sales.
2. The offering of free services for failure to penetrate the target is forbidden.
3. Public cracking, hacking, and trespass contests to promote security assurance for sales or marketing of security testing or security products are forbidden.
4. To name past or present clients in the marketing or sales for potential customers is only allowed if the work for the client was specifically the same as being marketed or sold and the named client has provided written permission to do so.
5. It is required that clients are advised truthfully and factually in regards to their security and security measures. Ignorance is not an excuse for dishonest consultancy.

#### B. Assessment / Estimate Delivery

6. Performing security tests against any scope without explicit written permission from the target owner or appropriate authority is strictly forbidden.
7. The security testing of obviously highly insecure and unstable systems, locations, and processes is forbidden until the proper security infrastructure has been put in place.

#### C. Contracts and Negotiations

8. With or without a Non-Disclosure Agreement contract, the security Analyst is required to provide confidentiality and non-disclosure of customer information and test results.
9. Contracts should limit liability to the cost of the job, unless malicious activity has been proven.
10. Contracts must clearly explain the limits and dangers of the security test as part of the statement of work.
11. In the case of remote testing, the contract must include the origin of the Analysts by address, telephone number or IP address.
12. The client must provide a signed statement which provides testing permission exempting the Analysts from trespass within the scope, and damages liability to the cost of the audit service with the exception where malicious activity has been proven.
13. Contracts must contain emergency contact names and phone numbers.
14. The contract must include clear, specific permissions for tests involving survivability failures, denial of service, process testing, and social engineering.
15. Contracts must contain the process for future contract and statement of work (SOW) changes.
16. Contracts must contain verified conflicts of interest for a factual security test and report.



### D. Scope Definition

17. The scope must be clearly defined contractually before verifying vulnerable services.
18. The audit must clearly explain the limits of any security tests according to the scope.

### E. Test Plan

19. The test plan may not contain plans, processes, techniques, or procedures which are outside the area of expertise or competence level of the Analyst.

### F. Test Process

20. The Analyst must respect and maintain the safety, health, welfare, and privacy of the public both within and outside the scope.
21. The Analyst must always operate within the law of the physical location(s) of the targets in addition to rules or laws governing the Analyst's test location.
22. To prevent temporary raises in security for the duration of the test, only notify key people about the testing. It is the client's judgment which discerns who the key people are; however, it is assumed that they will be information and policy gatekeepers, managers of security processes, incident response personnel, and security operations staff.
23. If necessary for privileged testing, the client must provide two, separate, access tokens whether they be passwords, certificates, secure ID numbers, badges, etc. and they should be typical to the users of the privileges being tested rather than especially empty or secure accesses.
24. When testing includes known privileges, the Analyst must first test without privileges (such as in a black box environment) prior to testing again with privileges.
25. The Analysts are required to know their tools, where the tools came from, how the tools work, and have them tested in a restricted test area before using the tools on the client organization.
26. The conduct of tests which are explicitly meant to test the denial of a service or process or survivability may only be done with explicit permission and only to the scope where no damage is done outside of the scope or the community in which the scope resides.
27. Tests involving people may only be performed on those identified in the scope and may not include private persons, customers, partners, associates, or other external entities without written permission from those entities.
28. Verified limitations, such as discovered breaches, vulnerabilities with known or high exploitation rates, vulnerabilities which are exploitable for full, unmonitored or untraceable access, or which may immediately endanger lives, discovered during testing must be reported to the customer with a practical solution as soon as they are found.
29. Any form of flood testing where a scope is overwhelmed from a larger and stronger source is forbidden over non-privately owned channels.
30. The Analyst may not leave the scope in a position of less actual security than it was when provided.



### G. Reporting

31. The Analyst must respect the privacy of all individuals and maintain their privacy for all results.
32. Results involving people untrained in security or non-security personnel may only be reported via non-identifying or statistical means.
33. The Analyst may not sign test results and audit reports in which they were not directly involved.
34. Reports must remain objective and without untruths or any personally directed malice.
35. Client notifications are required whenever the Analyst changes the testing plan, changes the source test venue, has low trust findings, or any testing problems have occurred. Notifications must be provided previous to running new, dangerous, or high traffic tests, and regular progress updates are required.
36. Where solutions and recommendations are included in the report, they must be valid and practical.
37. Reports must clearly mark all unknowns and anomalies.
38. Reports must clearly state both discovered successful and failed security measures and loss controls.
39. Reports must use only quantitative metrics for measuring security. These metrics must be based on facts and void of subjective interpretations.
40. The client must be notified when the report is being sent as to expect its arrival and to confirm receipt of delivery.
41. All communication channels for delivery of the report must be end to end confidential.
42. Results and reports may never be used for commercial gain beyond that of the interaction with the client.



### 2.5 The Operational Security Testing Process

Why test operations? Unfortunately, not everything works as configured. Not everyone behaves as trained. Therefore the truth of configuration and training is in the resulting operations. That's why we need to test operations.

The OpSec testing process is a discrete event test of a dynamic, stochastic system. This means that you will be making a chronological sequence of tests on a system that changes and does not always give the same output for the input provided. The target is a system, a collection of interacting and co-dependent processes which is also influenced by the stochastic environment it exists in. Being stochastic means the behavior of events in a system cannot be determined because the next environmental state can only be partially but not fully determined by the previous state. The system contains a finite but possibly extremely large number of variables and each change in variables may present an event and a change in state. Since the environment is stochastic, there is an element of randomness and there is no means for predetermining with certainty how all the variables will affect the system state.

Most of what people understand of OpSec comes from the defensive aspect which is understandable since security is generally considered a defensive strategy. Aggressive testing of OpSec is then relegated to the same class as the exploitation and circumvention of the current design or configuration. However, the fundamental problem with this technique is that a design or configuration does not equate to operation.

We encounter many instances in life where operation does not conform to configuration. A simple example is a typical job description. It is more common than not that the policy which dictates one's job, also known as a job description, falls short from actually reflecting what we do on the job. Another example is the TV channel. Because a channel is set to a particular frequency (configured) it does not mean we will receive the show broadcast on that channel or only that show.

This security testing methodology is designed on the principle of verifying the security of operations. While it may not always test processes and policy directly, a successful test of operations will allow for analysis of both direct and indirect data to study the gap between operations and processes. This will show the size of the rift between what management expects of operations from the processes they developed and what is really happening. More simply put, the Analyst's goal is to answer: "how do current operations work and how do they work differently from how management thinks they work?"

A point of note is the extensive research available on change control for processes to limit the amount of indeterminable events in a stochastic system. The Analyst will often attempt to exceed the constraints of change control and present "what if" scenarios which the change control implementers may not have considered. A thorough understanding of change control is essential for any Analyst.

An operational security test therefore requires thorough understanding of the testing process, choosing the correct type of test, recognizing the test channels and vectors, defining the scope according to the correct index, and applying the methodology properly.

Strangely, nowhere, besides in security testing is the echo process considered the defacto test. Like yelling into a cavernous area and awaiting the response, the echo process requires interacting and then monitoring emanations from the target for indicators of a particular state such as secure or insecure, vulnerable or protected, on or off, and left or right. The echo process is of a cause and effect type of verification. The Analyst makes the cause and analyzes the effect on the target. It is strange that this is the primary means of testing something as critical as security because although it makes for a very fast test, it is also highly prone to errors, some of which may be devastating to the target. Consider that in a security test using the echo process, a target that does not respond is considered secure. Following that logic, a target needs only to be non-responsive to a particular type of request to give the appearance of security



## OSSTMM 3 – The Open Source Security Testing Methodology Manual

however still be fully interactive with other types of requests which shows there has been no separation.

If hospitals used the echo process to determine the health of an individual, it would rarely help people, but at least the waiting room time would be very short. Hospitals however, like most other scientific industries, apply the Four Point Process which includes a function of the echo process called the "interaction" as one of the four tests. The other three tests are: the "inquest" of reading emanations from the patient such as pulse, blood pressure, and brain waves; the "intervention" of changing and stressing operating conditions such as the patient's homeostasis, behavior, routine, or comfort level; and the "induction" of examining the environment and how it may have affected the target such analyzing what the patient has interacted with, touched, eaten, drank, or breathed in. However, in security testing, the majority of tests are based on the echo process alone. There is so much information lost in such one-dimensional testing we should be thankful that the health care industry has evolved past just the "Does it hurt if I do this?" manner of diagnosis.

The security test process in this methodology does not recommend the echo process alone for reliable results. While the echo process may be used for certain, particular tests where the error margin is small and the increased efficiency allows for time to be moved to other time-intensive techniques, it is not recommended for tests outside of a deterministic environment. The Analyst must choose carefully when and under what conditions to apply the echo process.

While many testing processes exist, the Four Point Process for security testing is designed for optimum efficiency, accuracy, and thoroughness to assure test validity and minimize errors in uncontrolled and stochastic environments. It is optimized for real-world test scenarios outside of the lab. While it also uses agitation, it differs from the echo process in that it allows for determining more than one cause per effect and more than one effect per cause.

