REIKEN GROUP LLC

Reiken Group LLC

OPSEC Certification Roadmap

OPSEC Overview:

Operational Security (OPSEC) as a methodology was developed during the Vietnam War, when the U.S. military discovered that the enemy was using unclassified information (indicators) to obtain advance information on combat operations. It became apparent at that time that traditional information security programs were insufficient to deny critical information to the enemy. Since then, OPSEC has been used widely throughout the U.S. military and government. Reiken Group now brings OPSEC to the commercial workplace as an effective posture to protect confidential information and prevent vulnerability exploitation.

Traditional information assurance strategies begin with risk management where threats to information are examined from an inside-out perspective, identifying all perceived threats to key information assets. Although this approach can yield valid results, it can be overly labor intensive and runs the risk of missing components of the organization's information that is key to achieving business missions and strategic objectives. This often leads to an over-expenditure of resources for countermeasures while providing a false sense of security.

OPSEC provides a different approach where a connection is established between the organization's missions and information. The OPSEC approach uses an outside-in perspective to view the organization's missions through the eyes of an adversary. Using this perspective, an organization can implement more efficient and effective countermeasures to protect the mission.

OPSEC is an analytical process that accomplishes two primary objectives:

1. OPSEC denies an adversary access to unclassified indicators that reveal strategic intent, capabilities and critical information.
2. OPSEC allows managers to 'think like the wolf' and use techniques that identify vulnerabilities through the eyes of the adversary to provide strong countermeasures.

Organization's can seek OPSEC certification for the entire enterprise or a defined entity such as a business unit, department or business/client program.

Certification Process:

The roadmap to gaining OPSEC certification consists of three phases: The Learning Phase, the OPSEC Process Phase and the Stress Test Phase. Each phase provides a foundation for continuation to the next phase.

Phase 1 – The Learning Phase:

The Learning Phase is the foundation of the OPSEC program. In this phase, an OPSEC capability set is developed within the entity. Two training programs of instruction (POI) are delivered to staff, based on their roles within the entity or the enterprise.

The first POI is the Strategic OPSEC session. At least one executive member must undergo a one day (seven hour) Strategic OPSEC session. This provides an understanding of elements of OPSEC, threats to the organization, and deploying OPSEC from a strategic perspective. Strategic OPSEC training not only provides executive level understanding of OPSEC but also provides a perspective that management will leverage in the regulatory process and in sales/marketing and client relations initiatives.

The second POI is the OPSEC Practitioners Course. At least two members of the Operational team must undergo a five day (thirty hour) course. One of the individuals must be the person tasked with being the primary OPSEC practitioner for the entity. Personnel from business operations, security and information technology are ideal candidates for the course. The OPSEC Practitioners course is a comprehensive study session that provides a detailed introduction to OPSEC principles, the OPSEC 5 step cycle, and implementation of an OPSEC program in the workplace.

Phase 2 – The OPSEC Process Phase:

The OPSEC Process is a process with five components:

1. Identification of Mission Critical Information
2. Analyzing Deliberate and Inadvertent Threats
3. Analyzing Vulnerabilities from the Adversarial Perspective
4. Assessing the Risks
5. Applying Controls, Countermeasures and Deterrents

1. Identification of Mission Critical Information:

The first step, Identification of Mission Critical Information is driven by the mission criticality - how important the information is to the company or company clients. Mission Critical information is classified by sensitivity and importance based on how much the company (strategic and operational areas) rely on the information to carry out business operations. Mission critical information can be a client's customer data, proprietary company information and trade secrets or unclassified open source and internal information such as web site information, phone lists and personnel bios. The essence of mission critical information from an OPSEC perspective is information that is critical to the mission is of value to an adversary. In this component of the OPSEC process, the manager learns the skills to identify mission critical information.

2. Analyzing Deliberate and Inadvertent Threats:

The second step in the OPSEC Process is to analyze deliberate and inadvertent threats to the organization's mission(s). The effective identification of vulnerabilities requires a diligent understanding of the threats facing the entity. OPSEC Managers are introduced to adversarial collection capabilities and learn how to profile a full spectrum threatscape – profiling different types of threat sources, systematic and non-systematic threats; threat motivators and stimuli, and threat actions.

3. Analyzing Vulnerabilities from an Adversarial Perspective:

The third step in the OPSEC Process is to analyze the company's vulnerabilities using prioritized threat actions determined in Step 2 of the OPSEC Process. In this step, the manager learns adversarial strategies to identify vulnerabilities and indicators of value to the adversary. An understanding of adversarial strategies and the characteristics of indicators provides the manager with unique perspectives and capabilities for identifying information vulnerabilities. The manager will learn to apply intelligence principles such as signatures, associations, profiles, contrasts and exposure to identify where there are indicators of value to an adversary.

4. Assessing the Risks:

The fourth step in the OPSEC Process is to assess the risk facing the organization based on the likelihood and impact of vulnerability exploitation by a threat source. Managers will learn to use mission critical information, threat profiles and vulnerabilities to formulate risk tables and conduct a mission based risk assessment.

5. Implementing Controls, Countermeasures and Deterrents:

The final step in the OPSEC process provides the manager with the know-how to choose and implement Controls, Countermeasures and Deterrents (CCD's) to mitigate unacceptable risk elements. The manager is introduced to controls rationalization for deciding when to invest in CCD's vs. when to accept risk. An implementation strategy is learned for effective deployment of the OPSEC program within the workplace.

Phase 3 – Stress Test Phase:

The Stress Test Phase is a diagnostic account of how effectively the implemented OPSEC program neutralizes vulnerabilities and indicators. During this phase, Reiken Group experts conduct onsite OPSEC survey's to audit and grade the OPSEC program's readiness and effectiveness. Additional testing measures such as Red Team Exercises can be carried at the company's or client's request for stealthy evaluation of OPSEC awareness and readiness. Certification is awarded upon successful results of stress testing (standard stress testing does not include Red Team Exercises). If the entity fails to meet minimum requirements for certification, the deficits are detailed in a report which is provided to management. Reiken Group experts will return after a predetermined amount of time to stress test those elements of the program that initially failed. Successful completion of outstanding items will result in the award of the certification.