**Step by step internal assessment procedures**

Conducted annually, the general methodology of an internal assessment applies to all organizations, but specific procedures vary depending on mission focus. An effective internal assessment requires cooperation and participation from all hands since the assessment team, also known as the OWG members, may interview individuals, observe activities, and gather data during the course of the assessment. The OPSEC officer normally leads the assessment and the unit’s OWG performs the assessment activities. Small teams of individuals from within an organization, with or without assistance from other subject matter expert (SMEs), may also be used. The scope of an OPSEC assessment is usually limited to events and/or activities within the organization. Assessments focus on the organization’s routine daily operations or a specific operation, process, or activity. Though missions and functions of different commands vary, there are certain procedural similarities for conducting an assessment. There are three phases of the assessment process: planning, execution, and analysis and reporting.

* **Planning Phase**

Preparations for an assessment begin well in advance; the required lead-time depends on the nature and complexity of the operation or activities assessed (for example combat and peacetime operations). OPSEC officers ensure the planning phase includes sufficient time for a thorough review of pertinent processes, documentation, formal and informal coordination, and discussions. The steps of the planning phase include:

1. Determine the scope. This activity starts the planning phase and limits the assessment to manageable proportions and expectations. Consider geography, time, observation of units, and other practical matters. OPSEC officers identify which command activities, projects, processes, programs, or missions to assess.

2. Brief the commander. Depending on the command’s schedule and battle rhythm, OPSEC officers brief the assessment strategy to the commander. The in-brief includes the following information:

a. Purpose and scope. The purpose and scope includes any policy and requirements for the assessment. The purpose statement identifies potential vulnerabilities to command information and identifies mitigations to the vulnerabilities. OPSEC assessments are holistic and most likely cross into other security disciplines (e.g. personnel security, antiterrorism/force protection information security and physical security).

b. Team members. List assessment team members by name, department, primary function, and clearance status (if applicable).

c. Schedule. Provide a summary of the plan of action and milestones (POA&M) or schedule of events, highlighting the most significant events like the in-brief, events requiring external support, and out-brief.

d. Operational impact. Identify the timeframe and duration of the assessment. Identify planning considerations and operational factors for the chosen assessment period. Identify any impact to the crew (usually no impact) and impact to command operations and missions (usually no impact).

e. Administrative support requirements. List outside organizations providing support, like the NOST, Joint COMSEC Monitoring Activity (JCMA), or ISIC. Additionally, state if internal administrative support is required. For example, ensuring team members are available from each assigned department or division.

This website provides an example assessment in-brief and out-brief.

3. Select team members to augment the OWG (if required). Select team members for their analytical, observational, and problem-solving skills. OPSEC officers ensure team members represent the functional areas of intelligence, CI, security, communications, logistics, plans, cybersecurity, PA, contracting, acquisition, and administration if applicable. When appropriate, specialists from other functional areas, such as transportation or chemical, biological, radiological, and nuclear participate. At a minimum, working group and team members:

a. Become familiar with the assessment procedures and techniques, especially when team members do not have previous assessment experience.

b. Understand the assessed operation or activity.

c. Become familiar with the operation plan (OPLANs), orders, standard operating procedures (SOP), associated processes, and command policies/directives.

d. Know the command’s CIL for the mission. OPSEC officer reviews and validates critical information throughout the assessment.

e. Become familiar with the command’s threat assessment (TA) to include the adversary’s primary collection methods, goal, and objectives, intent, and capabilities.

f. Determine the command’s current or previous vulnerabilities; where or how the adversary may obtain critical information.

g. Develop functional outlines for respective areas of interest, knowing the “who, what, how, when, where, and why” of significant operational events that occur during an assessment. Command profiles are basic guides for this step. Command profiles or functional outlines provide a visual picture of an operation or command.

4. Analyze the adversary intelligence threat. Assessments, primarily conducted from the adversarial perspective, require a comprehensive and current all-source TA. Update the team on any changes to the adversary's intelligence capability and threat information especially, threats most relevant to their command.

5. Review empirical studies. Review empirical studies, such as COMSEC or CI reports. These reports simulate aspects of the adversary intelligence threat and support vulnerability findings.

* **Execution Phase**

Physical collection of information and data through observation of activities, personnel interviews, verifying command personnel follow policy, and collection of empirical data through open-source research and COMSEC monitoring reports are the primary actions conducted during the execution phase.

1. Data collection. Assessment team members must be alert to differences between what they read, what they assume to be the situation, what they learn from the command briefing, and what they observe. Expect conflicting data, team members adjudicate the data during the assessment period. A best practice is to assign a team member to lead an assessment area or function throughout the duration of the assessment. This provides the OPSEC officer the opportunity to monitor the assessment holistically, keep the assessment on track per the POA&M, and collect data from each team member at the end of each day.

a. Open source research (OSR). Conduct open source research to ensure the command is not publishing or posting critical information in publicly available information (PAI) environment. This includes reviewing the command’s public facing website, official social media pages, and a rudimentary search of what command members are posting online. The review also includes information contained in contracts, job announcements, Navy family ombudsman or readiness group pages, and any other information published to the public.

b. Administrative review. Conduct administrative reviews in order to determine if command members are following command policy. For example, if it is the command's policy to shred all printed paper products, then the assessment team should not find printed paper products in the trash or dumpsters. OPSEC and security policies can also include, the badging in/out process, quarterdeck procedures, visitor check procedures, recycling versus shred, burn bag procedures, encryption of e-mail, declaration of phone up/phone down practice, logging visitors in/out of classified spaces, and portable electronic device policy. The assessment team must know the policies and procedures in order to spot or observe a potential vulnerability.

c. Office, compartment, or space walk through. Assessment team members conduct a walkthrough of the organization offices, compartments, and spaces to identify potential OPSEC vulnerabilities and policy discrepancies. Team members check for items like phone stickers (DD Form 2056), operable shredders, computer screens facing windows, safes requiring repair or safes improperly unlocked, portable electronic devices in secure areas, classified or sensitive information requiring destruction (overflowing burn bags), passwords or safe combinations written down, etc. Team members document policy discrepancies and report security violations identified during the walk through.

d. Stand-off observations. Observation from a distance can reveal a lot about an organization and its personnel. If the adversary wants to gain access to an installation, they could conduct some level of surveillance, or standoff observations to look for a weakness or vulnerability in procedures. For example, the best opportunity to access a facility may be during heavy traffic (vehicle or foot) times, when security does their best to prevent jams or back-ups. Photographing of security badges when not secured or openly worn outside, making replication easier. Observing when doors are open, secured during the day, or whether or not “piggybacking” occurs, that can lead to easy access. The adversary may also observe if security cameras are present and functioning, and when watchstanders turnover.

e. Command member interviews/questionnaires. Talking to, or interviewing personnel about OPSEC can best define the command’s OPSEC culture. The Navy uses interviews (knowledge checks) to determine skill level and qualification status, and questionnaires (surveys) to determine command climate and various other reasons. The better the culture of OPSEC, the less likely vulnerabilities will exist. Interviews should be non-intrusive to command operations and personnel, short and concise, and tailored to the command’s mission, operation, or basic need for specific information. The percentage of interviews depends on the organization, but a best practice is roughly 25–30 percent. Sample interview questions are provided on this site.

f. Dumpster dives. We often take for granted or just turn a blind eye when it comes to determining what information we are potentially discarding. In years past, the messenger of the watch aboard every ship inspected trash prior to crossing the quarterdeck at the end of the day. Most shore organizations have all-shred policies, however seldom do commands verify members are following this policy. Because we typically do not review recycled paper for critical information, the recycling of whole paper has created an additional vulnerability. A best practice is for a member of the security department or OWG to check individual space trashcans at the end of the day for printed materials while conducting office, compartment, or space walk-throughs mentioned above. Commands can easily mitigate the vulnerability of placing discarded classified and critical information in the trash, by instituting and verifying all-shred policies. Commands can validate policies are being followed by periodically reviewing the trash during internal assessments or spot checks.

2. Findings. Report to the chain of command, for immediate mitigation or corrective action, any finding during the assessment considered to have a serious impact to the command’s mission or discovery of a security violation.

a. As previously stated, a best practice is to assign team members to lead an assessment area or function (OSR, observations, interviews, administrative review). At the end of each day, or earlier, the team leads report all findings to the OPSEC officer for consolidation and preparation of the assessment out-brief to the commander. Conduct end-of-day “hot wash” so team members can share, discuss, and adjudicate any findings.

b. A picture tells 1,000 words. Take photographs of findings (if possible) and include them in the final out-brief. Photograph discovered critical information, personally identifiable information (PII) or other printed material to highlight the vulnerability, while also protecting the PII and potential “violator”. Remember, internal assessments are non-attributional.

* **Analysis and Reporting Phase**

OPSEC officers and assessment teams compile, correlate, and analyze the collected data. The team identifies any potential vulnerabilities, poor OPSEC practices, other security violations and determines the command’s ability to protect critical information. The team recommends a countermeasure for each identified vulnerability. The OPSEC officer submits a final report or out-briefs the commanding officer on findings and countermeasure recommendations upon completion of this phase.

1. The final report or out-brief is usually in power point format, but is up to the command on what format or how to brief the commander. The report includes the command’s critical information and indicators, the adversary’s collection capabilities, vulnerabilities identified during the assessment, and recommended countermeasures. Although some vulnerabilities may be impossible to eliminate or mitigate, OPSEC officers include them in the report to enable the commander to assess fully the command, operation, or activity.

2. OPSEC officers track all findings until resolved. For example, if the vulnerability is personnel piggybacking or not badging properly, and the proposed countermeasure is to post a watch during high traffic times to monitor and inform personnel of proper procedures. This requires creating a schedule of who, when and where the watch takes place. Conditioning command members to properly badge in and out of the command only takes a few days. Discovering printed material in the dumpster and the proposed countermeasure is to conduct daily trash check. This is another example of how OPSEC officers can combat a vulnerability. Upon successful mitigation of the vulnerability, consider reducing the trash checks to once a week and then monthly.

3. Assessments are required annually; however maintain assessment findings for a minimum of three years in order to establish trends. Measures of performance (MOP) and measures of effectiveness (MOE) can also be established and even reported up the chain of command for best practices.