Vulnerability Assessment and Mitigation (VAM) methodology takes a top-down approach and seeks to uncover vulnerabilities that are known, in addition to vulnerabilities that exist yet have not been discovered or seen currently.

Overview of VAM:

1. Identify your organization's essential information function
2. Identify information systems essential to implementing the essential functions in step 1
3. Identify vulnerabilities of the essential systems in step 2
4. Identify pertinent security techniques to mitigate the vulnerabilities in step 3 using the VAM matching matrix tool
5. Select and apply techniques from step 4 based on constraints, costs, and benefits
6. Test the techniques applied in step 5 for robustness and actual feasibilities under threat
   1. Repeat steps 3 - 6 as needed

Operations Security (OPSEC)

Originated during Vietnam War. OPSEC is a countermeasures program for protecting critical information. OPSEC involves the following five steps:

1. Identify the critical information to be protected

* Critical information is any information the adversary needs to prevent our success - and that we must protect to ensure our success. Critical information includes items such as capabilities, intentions, times, places, locations, strengths, weakness, technology, and tactics (DoD)

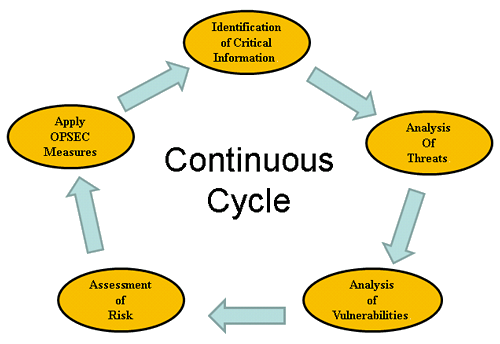
1. Analyze the threats

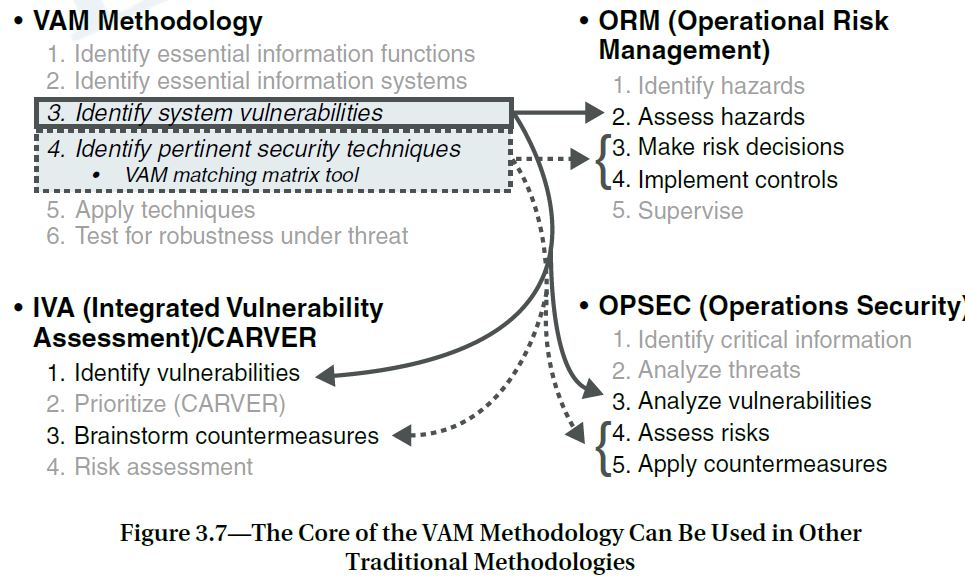
* Two elements of a threat = adversary intent to do harm, and capability to do you harm. If an adversary has intent to do you harm but do not have the means to get to you, you do not have a threat--currently. This can change rapidly.

1. Analyze vulnerabilities
   * Opportunities for adversaries = opportunities to exploit your critical information. Often indicators can point to vulnerabilities.
2. Assess risk
   * Three elements to risk: Threat x Vulnerability x Impact = Risk.
3. Apply countermeasures
   * Countermeasures need to be developed that eliminate the vulnerabilities, threats, or utility of the information to the adversaries. The countermeasures should include alternatives that may vary in effectiveness, feasibility and cost.

OPSEC in today's realm, needs to include protecting information from unfriendly eyes (need to know), industrial espionage, hackers, law enforcement, social engineering, and mass surveillance. You need to look at your organization through the eyes of your adversary. You need to put on the black hat and ask yourself, 'if I were a bad guy, could I use this information to harm the organization or disrupt the mission.' OPSEC is critical to our National Security.

OPSEC VAM





In conclusion, I would suggest using any number of the above VAM methodologies and then customizing them--picking and choosing, using part, some, or all of the methodologies to meet organizational or security posture goals. This is a way to improve upon one single method.

Work Cited

"Operations Security." *Operations Security - Wikipedia, the Free Encyclopedia*. n.d. Web. <https://en.wikipedia.org/wiki/Operations\_security>.

n.d.DoDEA. *Operations Security (OPSEC)*. Retrieved from http://www.dodea.edu/Offices/Safety/OPSEC.cfm