Webinar Questions and Answers

Risk Management—Assessing Risks

Webinar guests submitted several questions before and during the January 9, 2014 Risk Management—Assessing Risks session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: How is the risk management process different than the OPSEC process?

Answer: Both are very similar since they require the following to be conducted: criticality, threat, vulnerability, and risk assessments. However, the OPSEC process is specific in terms of critical information while CDSE's Risk Management model gives a broader view of the Risk Management process itself.

Question: Are there any websites for best business practices?

Answer: DoD addresses risk management in several policy documents from acquisitions, and antiterrorism to OPSEC. Currently we are unaware of a DoD website that addresses best business practices for risk management. However, any information related to the Federal Information Security Management Act (FISMA) can be found at http://www.rmf.org/.

Question: Is Defense Security Service (DSS) going to ask for this during our review?

Answer: Please refer to you Industrial Security Representative.

Question: Would the outcome of the assessment be included in a business continuity plan or Emergency disaster plan?

Answer: Yes, however, it is important that when discussing and or documenting vulnerabilities and countermeasures associated with the protection of an asset, to make this information more sensitive and in some cases classified. The information must be kept as a separate annex apart from other plans and restricted to persons with the need to know. Recommend coordinating with your local security office to determine the sensitivity or classification of any vulnerabilities related to the assessment prior to publishing them.