

Webinar Questions and Answers

DSS Risk Management Framework Overview

Webinar guests submitted several questions before and during the August 14, 2014 DSS Risk Management Framework Overview session. The following responses are provided by the Center for Development of Security Excellence (CDSE).

Question: “We are awaiting Army's implementation policy. Curious as to how quickly other DoD agencies are adopting this as of today.”

Answer: DoD has identified a transition timeline for DoD IT systems that is dependent upon system authorization status. For the most part, systems at either the beginning or end of their lifecycle (those that are either brand new and unaccredited, or reaching the end of their three year accreditation period) will need to transition to the RMF process within the next six months. Systems that are currently accredited will be part of a planned transition process. Regardless of status, you should immediately begin planning to transition to the RMF. Consult the RMF knowledge service for more information. The link is provided in our RMF Overview Resource handout.

Question: When will RMF for DoD IT will be applied for Cleared Contractor Information Systems?

Answer: CDSE does not have the authority to state when and how the Risk Management Framework will become part of the NISP C&A Process, but that it is likely that many elements will eventually be included. In the meantime, cleared industry's customer (DoD) is making this transition now, and as part of RMF, will look to include Industrial Security as a partner in enterprise wide risk management.

Question: What is the role of a security officer in RMF?

Answer: The updated DoD Cybersecurity Policy, particularly DODI 8510.01 Risk Management Framework, recognizes the value of, and mandates that we include all security disciplines in the cybersecurity process. Security personnel, whether physical security, information security, personnel security, or industrial security, have a knowledge of the threat environment for information systems from the physical location to the users themselves. Security personnel also have knowledge of the processes and requirements for the use of the information systems that can help identify vulnerabilities. This knowledge is critical for identifying and configuring systems, determining appropriate security controls, and implementing continuous monitoring. Full participation of all security disciplines will be the key to the success of the Risk Management Framework.

Question: How does RMF apply to a contractor that only accesses JPAS to manage personnel security? Does it apply to our entire company intranet or just the devices that interact with JPAS?

Answer: Contractors who only access JPAS to manage personnel security do not have any requirements under RMF.