DISA
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DISA Risk Management Framework – Service Product Packages

Under the Defense Information Assurance Certification and Accreditation Process (DIACAP), the roles and responsibilities for controls and evidence requirements were not always clear or accessible. To address these gaps and issues, the Defense Information Systems Agency (DISA) executed a plan to increase service delivery through streamlined Risk Management Framework (RMF) processes and readily accessible evidence based on mission partner requirements. The outcome of the plan resulted in five DISA RMF Service Product Packages.

DISA Service Product Packages are "Assess Only" packages which are comprised of comprehensive security test and/or assessment results for "reuse" by leveraging organizations, providing its own authorizing official (AO) a holistic view of their associated information systems' risk posture. These packages contain Control Correlation Identifiers (CCIs) which have been validated and assessed as "inherited" and/or "shared" between DISA and the mission partner. These packages are assessed by the DISA Security Control Assessor (SCA).

The term "*reuse"* is defined as the leveraging of another organization's security assessments in order to reuse that information to support a similar package. In some cases (e.g., when separate organizations have similar mission requirements), an organization may want to leverage an existing authorization or "Assess Only" package that is provided by a separate organization. In these cases, the leveraging organization becomes the information system owner and must authorize the system through the complete RMF process, but uses completed test and assessment results provided to the leveraging organization to the extent possible to support the new authorization by its own AO. Reuse is considered a form of reciprocity because it relies on acceptance of testing and assessment conducted by organizations other than the one authorizing the system in question. Such reuse will represent significant resource savings to the leveraging organization.

The DISA Service Product Packages are available to mission partners who have programs and systems hosted within DISA datacenters. Mission partners will select ONE service product package to inherit based on elected services. The CCIs will be "shared" and/or "inheritable" and will gradually increase based on elected services. These packages are all-inclusive meaning the mission partner will inherit from a baseline package and additional services purchased. A detailed list of shared and inheritable CCIs per package can be found in the DISA Terms and Conditions.

Below is the DISA RMF Service Product Packages matrix which provides a high-level overview of each available package.

DISA
DEFENSE INFORMATION SYSTEMS AGENCY
The IT Combat Support Agency

DISA Risk Management Framework – Service Product Packages

DISA RMF Service Product Packages Matrix

Function	PACKAGE 1 OS Only	PACKAGE 2 OS + Partial Application	PACKAGE 3 OS + Entire Application	PACKAGE 4 OS Only VOE Only	PACKAGE 5* OS + Entire Application (VOE Only)
DISA AOR	Manages OS	Manages OS + one platform	Manages OS + all platforms	Manages OS (MP-directed configurations)	Manages OS + all platforms (MP-directed configurations)
Patch Management	No authority to patch at will; PM approves	No authority to patch at will; PM approves	No authority to patch at will; PM approves	DISA secures at will due to automation of restore/provisioning	DISA secures at will due to automation of restore/provisioning
Control/CCI Responsibility (Leans Towards)	Shared or MP	Shared	Shared	Inheritable or shared	Inheritable or shared
DISA Package Type	Assess Only	Assess Only	Assess Only	Assess Only	Assess Only
AO	MP	MP	MP	MP	MP

AOR	Area of Responsibility	**OS**	Operating System
CCI	Control Correlation Identifier	**PM**	Program Manager
DISA	Defense Information Systems Agency	**VOE**	Virtual Operating System
MP	Mission Partner		

SPECIAL NOTE: When electing Package 5 (OS + Entire Application [VOE Only]) the mission partner will not have privileged access and will be responsible for application design and development (e.g., coding, testing, etc.).

Mission partner system-specific Patch/Security Technical Implementation Guide (STIG) CCIs will not be inheritable; however, the mission partner will have visibility of their data via the Enterprise Security Posture System (ESPS). A DD Form 2875 is required. The URL to request access is as follows:

ESPS Account: https://esps.csd.disa.mil/main.asp