DISA Risk Management Framework (RMF)

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, DISA executed a plan to increase service delivery through streamlined RMF processes and readily accessible evidence based on mission partner requirements. This plan includes an inheritance model for RMF to ensure that mission partners will have transparency into the facility, network, and services that are being delivered by DISA in support of mission partner workload. Each of these components, as described below, provides the building blocks necessary to support authorization of the systems' operated within the DISA Ecosystem.

The **DISA Inherited Policy (DIP) Package** is an "Assess Only" package which contains DOD Chief Information Officer (CIO) and DISA policy/guidance controls assessed and validated as "common" and/or "shared" between DISA and the mission partner.

The **DISA Datacenter Packages** are assessed and authorized packages which contain "common" physical and environmental controls for inheritance by DISA and customers who have programs and systems hosted within DISA datacenters and field activities. These packages are authorized by the DISA Authorizing Official (AO).

The **DISA Network Package** is an assessed and authorized package which contain "common" transport and network infrastructure controls available for inheritance by DISA and customers who utilize the DISA Computing Ecosystem Command Circuit Service Designators (CCSDs) to transport and receive program and system information. This package is authorized by the DISA AO.

The **DISA Service Product Packages** are "Assess Only" packages which are comprised of comprehensive security test and/or assessment results for "reuse" by leveraging organizations, giving its own AO a holistic view of their associated information systems' risk posture. Five packages have been defined equating to the level of services desired by the mission partner. Each package contains Control Correlation Identifier (CCIs) which have been assessed and validated as "inherited" and/or "shared" between DISA and the mission partner. These packages are validated by the DISA Security Control Assessor (SCA).

The term "r*euse"* is defined as 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 assessments conducted by organizations other than the one authorizing the system in question. Reuse does not require agreements between the subscriber and provider organizations. Such reuse will represent significant resource savings to the leveraging organization.

DISA Risk Management Framework (RMF)

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 Packages 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.

DISA 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 Mission Partner	Shared	Shared	Inheritable or Shared	Inheritable or Shared
DISA Package Type	Assess Only	Assess Only	Assess Only	Assess Only	Assess Only
Authorizing Official	Mission Partner	Mission Partner	Mission Partner	Mission Partner	Mission Partner

DISA will provide mission partner awareness training on the RMF Service Product Packages on: September 19, 21, 26 and 28 from 1400-1500 EDT.

DCS link: https://conference.apps.mil/webconf/CyberControlSection
Conference line: 301-909-7350 PIN 34720974#