



*The **IDRMP Module** is a risk assessment module within EPRM to facilitate assessments used by commanders, Integrated Defense Working Groups, and defense planners with data to make more informed decisions concerning the defensive posture of the installation. Implementing the tool's process model for characterizing the organization, identifying the organization's critical assets, assessing the threats, and assessing the benchmarks, users are able to create an assessment in a standardized risk framework.*

Department of Defense (DoD) Directive 3020.40, Mission Assurance (MA), directs the Services to integrate mission assurance assessment information into risk-assessment and risk-management activities. It develops a DoD-wide process to assess and manage risk and provides the authority for the Joint Staff to designate a system of record for conducting the assessments down to installation and tenant level. Additionally, DoD Instruction O-2000.16, Volume I, DoD Antiterrorism (AT) Program Implementation: DoD AT Standards, implements mandatory AT program elements within the mission assurance construct. Consistent with the DoD guidance, Air Force Instruction (AFI) 31-101, Integrated Defense (ID), requires Installation Commanders to identify and mitigate risk impacting operations, personnel, and resources. It also describes the methodology for implementation as the Integrated Defense Risk Management Process. In March of 2018, the Joint Staff designated the Enterprise Protection Risk Management (EPRM) tool as the Mission Assurance System of Record for risk assessment data.

Alion 11/22

The Integrated Defense Risk Management Process (IDRMP) Module—

DATA COLLECTION

The assessment is divided into several process steps, described below. The current step will be indicated with a “Click Here” medallion. A green check mark medallion indicates the section is completed, and a lock medallion means the section is not available until the current section is completed.



PROFILE ORGANIZATION—

Describes the organization being assessed



SCOPE ASSESSMENT—

By design, these questions determine the breadth of assessment questions to be completed by the unit/installation (e.g. if a unit does not possess classified information, a “no” answer to this question will eliminate questions regarding classified information from the assessment).



IDENTIFY ASSETS—

284 asset types are organized into 12 categories. Select assets applicable to the assessment. This section is typically pre-filled from the inherited pre-scored asset template. Complete any unanswered questions and make necessary adjustments to an asset's criticality score, as needed, based on known local data.



CHARACTERIZE THREATS—

48 threat scenarios are comprised of 6 threat sources and 22 threat methods. Select threats applicable to the assessment. This section is typically pre-filled from the inherited AHTA (Service or DIA baseline). Complete any unanswered questions and make necessary adjustments to a threat's rating, as needed, based on known local data.



CONDUCT ASSESSMENT—

263 benchmark questions are organized into 14 categories.

RESOURCES

The IDRMP benchmarks were developed in a collaborative working group in place as a technical advisory resource to guide the overall development of the IDRMP module for the EPRM tool. In addition, the working group provided subject matter expertise in developing the content of the IDRMP module. The goal of the working group was to ensure the resulting tool set meets the needs of Air Force IDRMP practitioners and stakeholders. The working group relied on the following two resources for the development of the IDRMP benchmarks.

THE 2018 DOD MISSION ASSURANCE ASSESSMENT BENCHMARKS— provide the basis for conducting mission assurance assessments throughout the DoD. These benchmarks support the broadly stated standards defined in various DoD directives, instructions, manuals, and other Federal standards setting directives.

THE 2018 DEFENSE THREAT REDUCTION AGENCY DOD MISSION ASSURANCE ASSESSMENT (MAA) GUIDELINES— provide the basis for conducting MAAs throughout the DoD. These benchmarks support the broadly stated standards defined in various DoD directives, instructions, manuals, and other Federal standard setting directives. These benchmarks are supplemented by the DTRA MAA Guidelines, which contain recommended questions for assessors to ask in order to find potential vulnerabilities in each benchmark. DoD Benchmarks are the base standard required for all MAAs. Services, components, and combatant commands may add specific requirements and resources to the DoD Benchmarks and publish their own benchmarks for use by their respective MAA teams.



EPRM
Enterprise Protection
Risk Management

Need assistance or want to provide
feedback?

Contact EPRM User Support:

EPRMhelp@HII-TSD.com

or

800.754.4204

(0700-1700 EST, M-F)

Additional Resources:

View user guides, videos, & training:

<http://eprmhelp.countermeasures.com/>



Save Time

CREATE A TEMPLATE — The Templates featured in EPRM allow Template Managers to create a set of pre-loaded answers or values that can be inherited when an Assessor creates a new assessment. The template is a way to provide common answers, or a baseline for multiple organizational assessments. Unlike assessments, not all questions must be addressed and a template can be used for a single focus, like threat characterization.

COPY FROM A PREVIOUS ASSESSMENT — The “copy from” feature allows users to copy answers from an existing assessment into a new assessment. This saves time when conducting a recurring, periodic assessment. The Assessor still has the ability to modify the copied answers if circumstances have changed since the last assessment period, but they do not need to answer all the questions over again.

Show Metrics

GENERATE ASSESSMENT REPORT — Once an assessment is completed and locked, click the Reports button in the Assessment Administration window to access hyperlinks for various report documents, analysis spreadsheets, and presentations based on the selected assessment.

GENERATE MULTI-ASSESSMENT REPORT — EPRM provides users with two options for analyzing multiple assessments in aggregate. Click the Advanced Analysis button

Administration

SHARE AN ASSESSMENT — Users may provide access to an assessment to other users within their objective hierarchy. Users sharing assessments set the level of access to “Read/Write” or “Read Only”.

CHANGE ASSESSMENT OWNER — Users may transfer ownership of their assessment to any other user within their objective hierarchy. Once changed, the original owner no longer has any access to the assessment.



DUPLICATE AN EXISTING ASSET — Users can create additional assets as long as the type of asset is already in the assessment. For example, if it was necessary to differentiate two types of Secret information, users could create a duplicate Secret information asset and give different names to each. Utilize the Duplicate Asset button to add a copy of the selected asset.

EXPORT/IMPORT CHECKLISTS — Depending on the speed of local SIPRNET connections, an Assessor may benefit from exporting the Countermeasures checklist as a Microsoft Excel document. Once in Excel, the checklist can be completed on the PC or printed to be completed manually. Once the checklist is complete, Assessors utilize the Upload Responses button to import the checklist back into EPRM.

to enter the Advanced Analysis screen. Scroll down to the bottom of the page and leave a check (✓) mark next to the individual assessments to be included in the analysis. Or, to conduct analysis for all assessments conducted on a particular node, utilize the “Select Nodes for Analysis” button above the Completed Assessments grid. Leave a check (✓) mark next to the node to be compiled. Users must click the “Apply Node Filter” button to apply the node selection. Regardless of which method is chosen, click the “Continue with Selected Assessments” button to run the analysis.

ARCHIVE AN ASSESSMENT — If the Started and Completed Assessments list contains more items than desired, users can move assessments to the Archive tab to hold them separate from the Active assessments. The same process works in reverse, if necessary.