EPRM
Enterprise Protection Risk Management

The IP module

is comprised of Information, Personnel and Industrial Security countermeasures. The purpose of the module is to automate Information Protection assessments and allow senior leaders to receive trend analysis. The module consists of 60 Information Security questions, 19 Personnel Security questions, and 11 Industrial Security questions for a total of 90.

AFI 16-1404 mandates that AF unit information, personnel and security assessments are conducted using EPRM. EPRM replaces the Management Internal Control Tool (MICT) for AF IP inspections.

Information Protection self-inspections are required to be conducted annually by the end of the fiscal year in accordance with DoD Memo 5200.01.

EPRM allows users to customize their assessments for their unit. For example, if a unit does not have any aircraft assets, the unit will not need to address countermeasure questions regarding aircraft assets. This saves time by allowing the users to focus on items pertaining to their unit and eliminates the need to have 'N/A' responses.

EPRM - Information Protection module

DATA COLLECTION

PROFILE ORGANIZATION—

Most questions in this section are data call questions with no impact to the remaining assessment questions for assets, threats, or benchmarks. Typically, wing assessments are conducted every 3 years. Self assessments are conducted annually (DoDM 5200.01). In future iterations of EPRM, the regional selection will apply varying threat profiles. The tenant organization question will trigger additional benchmark questions if answered positively. Use the facility comments area to leave any pertinent information regarding the assessment being conducted.

SCOPE ASSESSMENT—

All questions in this section are linked to countermeasure questions on the Conduct Assessment/ countermeasures page. Answering 'no' to any question will filter out related countermeasure questions from the Conduct Assessment page. For example, if the assessor answers 'no' to having Classified Information Systems, they will not see countermeasure questions related to Classified Information Systems in the checklist. This filtering function streamlines the checklist and saves the unit time and resources.

IDENTIFY ASSETS—

The DoD Information Security Program implements guidance for classification and declassification of DoD information that requires protection in the interest of national security. The specific information assets include: SCI, Top Secret, Secret, Confidential, NATO, Formerly Restricted Data, Restricted Data, Critical Nuclear Weapons Design Information, SIGMA, and Controlled Unclassified Information. These assets were compiled from DoD policy issuances DoDM 5200.01, volumes 1-4.

CHARACTERIZE THREATS—

When evaluating a threat a combination of a threat source and a threat method are considered. The IP module provides the following source and method pairings to consider when conducting an IP assessment.

THREAT SOURCE:	THREAT METHOD:
Criminals	HUMINT and Open Source
Insiders	HUMINT and Negligent Disclosure
Non-state Actors	HUMINT and Open Source and SIGINT
State Actors	HUMINT and Open Source and SIGINT

CONDUCT ASSESSMENT—

Checklist questions are comprehensive and designed to ensure the activity security manager is competent in the subject areas. Checklist questions were compiled from the following references:

DoD 5220.22-R	DoDM 5200.45	AFI 16-1404
DoDM 5200.02	DoDD 5210.50	AFI 16-1406
DoDI 5210.02	DoDI 5210.83	AFMAN 13-501,
DoD 5210.42	USSAN 1-07	DoDM 5200.01, vol. 1-4

The IP Checklist Composition

Information Security: 60 questions based on six of seven self-inspection report categories (OCA, Security Violation, Management, Marking, Access, and Safeguarding).

Personnel Security: 19 questions focused on highest risk personnel. Continuous evaluation program rated as the highest risk. No questions on DoD HSPD-12 and suitability.

Industrial Security: 11 questions regarding Visitor Group Security Agreement (VGSA), cleared facilities and DD 254 related questions. No questions on contractor's suitability.

EPRM
Enterprise Protection Risk Management

Need assistance or want to provide feedback?
Contact EPRM User Support:
EPRMhelp@alionscience.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.

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.

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 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.

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.

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.