EPRM

Enterprise Protection Risk Management

The ISC Module

The Interagency Security Council (ISC) Risk Management Process (RMP), consistent with Executive Order 12977 and amended by Executive Order 13286, is intended to be applied to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities to include: existing owned, to be purchased or leased facilities, stand-alone facilities, Federal campuses, individual facilities in Federal Campuses, and special use facilities.

The RMP defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level (FSL), and provides an integrated, single source of physical security countermeasures for all Federal facilities. The standard further provides guidance for customization of the countermeasures for facilities and the integration of new standards and concepts contained in the Interagency Security Committee's (ISC) published guidelines.

EPRM administers the results from the RMP in one simple analysis, identifying areas of wasted resources that can be applied to unmitigated risks. For a more comprehensive and granular approach, the software also includes its own analysis, taking a deeper look into the assessment results.

Alion 3/20

EPRM - The Interagency Security Council module

DATA COLLECTION

PROFILE ORGANIZATION—

This section is used to record the Facility Security Level (FSL) Determination for the facility being assessed. Elements taken into account are facility's Mission Criticality, Symbolism, Population, Size, and perceived threat to Tenant Agencies. Facilities with childcare centers will automatically be scored "very high" and given a 4 point score with respect to the facility population.

SCOPE ASSESSMENT—

The FSL level may be adjusted up or down one level based on the intangibles of the facility. Consideration should be given for a Level V designation if a "very high" score is valued for criticality or symbolism, and is a one-of-a-kind facility (or nearly so), regardless of Level designation. A justification comment is required for any adjustments to the FSL.

IDENTIFY ASSETS—

This section contains only one question and requires the assessor to affirm and assign a value to the facility in order to continue. The assessor's valuation is subjectively based on the target value of the building or facility.

CHARACTERIZE THREATS—

The ISC module contains 35 Undesirable Events (UEs) to be evaluated. Each UE carries a default rating as identified in Appendix A: Design-Basis Threat (DBT) report. The DBT establishes the characteristics of the threat environment to be used in conjunction with all ISC physical security standards. When evaluating UEs, the assessor may consider local threat data to modify the default rating. Any modifications to the default rating must be accompanied by a justification comment.

Countermeasure questions are derived from the following security criterion:

THREAT SOURCE:	THREAT METHOD:
Cyber Security	Facility Entrance Security
Interior Security	Security Operations & Administration
Site Security	Structure Security
Systems Security	

CONDUCT ASSESSMENT—

Risks to a facility must first be identified and assessed in order to determine the necessary level of protection (LOP). Assessors must answer all countermeasure questions in order to complete the data collection phase of the assessment. As a result, the assessed risk may reveal not only the facility's unmitigated risks, but wasted resources as well.

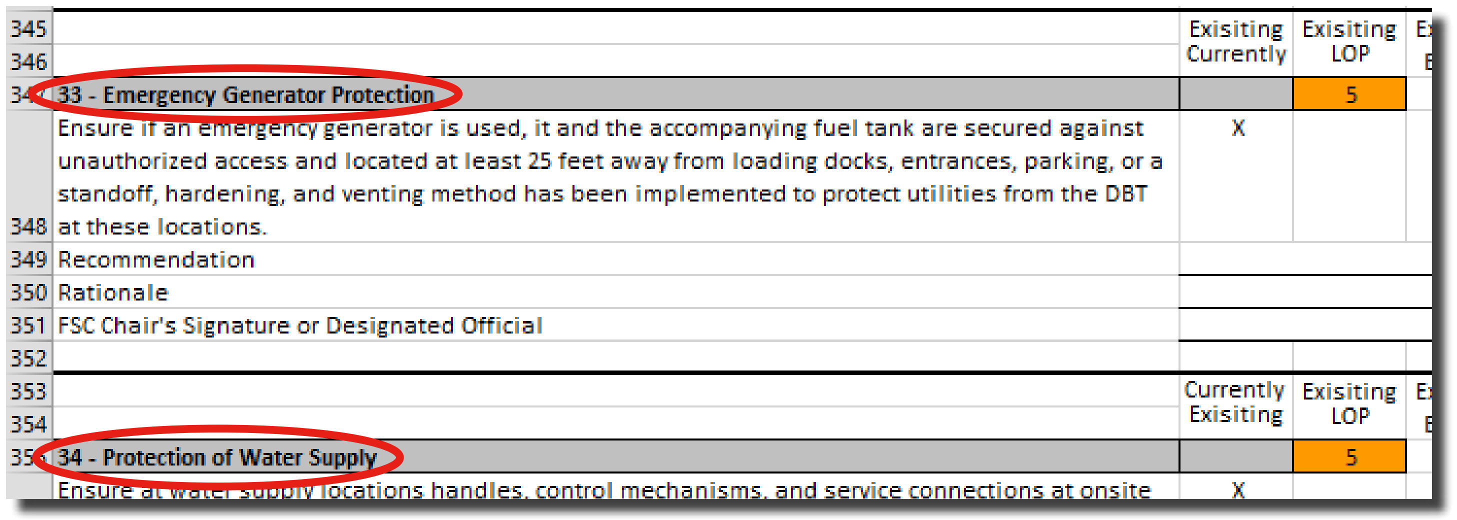
RESOURCES—

The ISC module was created from the following sources:

- The Risk Management Process for Federal Facilities
- RMP Appendix A: The Design-Basis
- Threat Report
- RMP Appendix B: Countermeasures
- RMP Appendix C: Child Care Centers

REPORTING—

Within the EPRM generated report, "ISC Levels of Protection by Security Criteria", each numbered site security criterion is identical to the site security criteria in the RMP Appendix B: Countermeasures resource. The report is arranged to display countermeasures in an order of increasing LOP. Those countermeasures that are in place already will be marked with an "X". The Existing LOP, sum of in place countermeasures Level 1 – Level 5, will be highlighted on the page.



345		Exisiting Currently	Exisiting LOP	Ex
346				
34	33 - Emergency Generator Protection		5	
348	Ensure if an emergency generator is used, it and the accompanying fuel tank are secured against unauthorized access and located at least 25 feet away from loading docks, entrances, parking, or a standoff, hardening, and venting method has been implemented to protect utilities from the DBT at these locations.	X		
349	Recommendation			
350	Rationale			
351	FSC Chair's Signature or Designated Official			
352				
353		Currently Exisiting	Exisiting LOP	Ex
354				
35	34 - Protection of Water Supply		5	
	Ensure at water supply locations handles, control mechanisms, and service connections at onsite	X		

HTTP://EPRMHELP.COUNTERMEASURES.COM/

ALION

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.