EPRM
Enterprise Protection Risk Management

The USAF PKI Audit Survey Module

The EPRM Cyber Module (ECM) for AF LRA PKI Audits is a survey module within EPRM to facilitate annual compliance audit inspections as detailed in the DoD PKI Registration Authority (RA) / Local Registration Authority (LRA) Certification and Registration Practice Statement (DoD PKI RA/LRA CPS/ RPS). The audit survey provides PKI auditors higher audit efficiency, integrated training resources, while reducing workload capacity. Additionally, the automation of audit checklists further enables the capability to facilitate remote/virtual completion of a PKI audit by AF site/ installation/base personnel.

Legacy AFMAN 17-1301 (Feb 2017)(being replaced by AFMAN 17-1304; currently in draft) directs all AF LRA to complete the AF LRA PKI Self-Assessment and send the results to the AFPKI RA on an annual basis. Access to trends analysis and reporting are easily accessible to the relevant PKI authorities positioned atop the hierarchy chain within the EPRM tool.

Alion 5/20

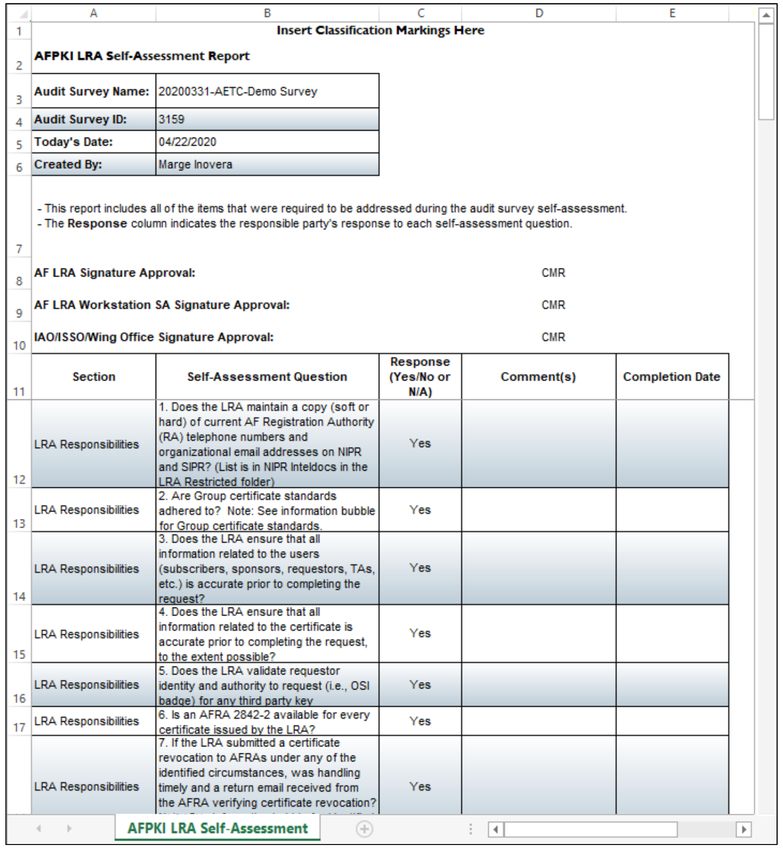
DATA COLLECTION

PROFILE ORGANIZATION—
An RA Officer operating under the RPS requires the services of at least one Local Registration Authority (LRA), an LRA Systems Administrator (SA), and an Information Assurance Officer (IAO). Coordinated by the LRA, the audit survey will be completed by these respective authorities and compiled back into the PKI Audit Survey Module. Each question requires a 'yes' or 'no' answer and comments are required for any 'yes' answers. Comment guidelines accompany each question.

LRA RESPONSIBILITIES & PHYSICAL CONTROLS—
31 questions regarding physical controls and security checks, proper documentation, storage and archiving procedures, and certificate and workstation standards.

RESOURCES—
- Legacy AFMAN 17-1301 (Feb 2017): implements computer security in support of Air Force Policy Directive (AFPD) 17-1, and Air Force Instruction (AFI) 17-130.
- CNSSI 1300: states the policy and security requirements for issuing and managing certificates issued by the NSS PKI DoD Certification Authorities (CAs). NSS PKI members can rely on these policy and security requirements to establish and maintain assurance in a certificate issued by a NSS PKI CA.
- DoD Registration Practice Statement: NSS PKI implementation instructions for RAs and TAs to maintain compliance with CNSSI 1300 (Instruction for National Security Systems Public Key Infrastructure X.509).
- DoD PKI RA/LRA Certification Practice Statement: defines the practices, policies and procedures under which the DoD RAs and LRAs operate.
- DoD X.509 Certificate Policy: defines the requirements for the creation and management of Version 3 X.509 public key certificates for use in applications requiring communication between networked computer-based systems.

REPORTING—
A full recounting of the LRA Audit Survey is available in a single report. Report data is presented in an Excel format, organized by the individual areas of responsibility for the LRA, LRA Workstation System Administrator, and the IAO/Wing/ISSO Cyber Security elements. The report captures all responses, comments, and completion dates in one concise document.



Insert Classification Markings Here

AFPKI LRA Self-Assessment Report

Audit Survey Name:	20200331-AETC-Demo Survey
Audit Survey ID:	3159
Today's Date:	04/22/2020
Created By:	Marge Inovera

- This report includes all of the items that were required to be addressed during the audit survey self-assessment.
- The **Response** column indicates the responsible party's response to each self-assessment question.

AF LRA Signature Approval: CMR

AF LRA Workstation SA Signature Approval: CMR

IAO/ISSO/Wing Office Signature Approval: CMR

Section	Self-Assessment Question	Response (Yes/No or N/A)	Comment(s)	Completion Date
LRA Responsibilities	1. Does the LRA maintain a copy (soft or hard) of current AF Registration Authority (RA) telephone numbers and organizational email addresses on NIPR and SIPR? (List is in NIPR Inteldocs in the LRA Restricted folder)	Yes		
LRA Responsibilities	2. Are Group certificate standards adhered to? Note: See information bubble for Group certificate standards.	Yes		
LRA Responsibilities	3. Does the LRA ensure that all information related to the users (subscribers, sponsors, requestors, TAs, etc.) is accurate prior to completing the request?	Yes		
LRA Responsibilities	4. Does the LRA ensure that all information related to the certificate is accurate prior to completing the request, to the extent possible?	Yes		
LRA Responsibilities	5. Does the LRA validate requestor identity and authority to request (i.e., OSI badge) for any third party key	Yes		
LRA Responsibilities	6. Is an AFRA 2842-2 available for every certificate issued by the LRA?	Yes		
LRA Responsibilities	7. If the LRA submitted a certificate revocation to AFRAs under any of the identified circumstances, was handling timely and a return email received from the AFRA verifying certificate revocation?	Yes		

AFPKI LRA Self-Assessment

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.