**Statewide Health Information Policy Manual (SHIPM) 3.1.6 – Security Evaluations**

*Compliance Review Tool Question #52*

## Artifact Must Haves

| **Item #** | **Topic** | **Covered (Y or N)** | **Comment** |
| --- | --- | --- | --- |
| 1 | Did the organization submit an artifact(s) regarding how they perform Security Evaluations? | Y🞏 N🞏 |  |
| 2 | Does the artifact(s) describe the process/guidelines/methodology use to perform Security Evaluations, as follow: |  |  |
| 2a | * Identify the scope of the analysis?
 | Y🞏 N🞏 |  |
| 2b | * Gather data?
 | Y🞏 N🞏 |  |
| 2c | * Identify and document potential threats and vulnerabilities (including probability and consequences)?
 | Y🞏 N🞏 |  |
| 2d | * Assess current security measures?
 | Y🞏 N🞏 |  |
| 2e | * Document the results of a vunerability scan?
 | Y🞏 N🞏 |  |
| 2f | * Was the last vunerability scan performed within the last two years?
 | Y🞏 N🞏 |  |
| 2g | * Determine the potential impact of identified vunerabilities?
 | Y🞏 N🞏 |  |
| 2h | * Determine the level of risk?
 | Y🞏 N🞏 |  |
| 3 | Does the artifact(s) identify the assets (system and facility) that are at risk? | Y🞏 N🞏 |  |
| 4 | Does the artifact(s) provide the identification and estimation of cost of protective measures that would eliminate or reduce the vulnerabilities to an acceptable level? | Y🞏 N🞏 |  |
| 5 | Does the artifact(s) describe the process to address vunerabilities in the Security Evaluation in a timely manner? | Y🞏 N🞏 |  |
| 6 | Does the artifact(s) describe how to communicate the results of the Security Evaluation to organization leadership? | Y🞏 N🞏 |  |
| 7 | Does the artifact(s) have official review/acceptance: |  |  |
| 7a | * Effective Date?
 | Y🞏 N🞏 |  |
| 7b | * Revision Date?
 | Y🞏 N🞏 |  |
| 7c | * Authorizing Sr. / Executive Management Signature?
 | Y🞏 N🞏 |  |

Title(s) of Submitted Policy/Document/Artifact(s) Reviewed:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Stored Location of, or link to Artifact(s) Reviewed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Overall CalOHII Reviewer Comments:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Name of CalOHII Reviewer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date Reviewed: \_\_\_\_\_\_\_\_\_\_\_\_

Title of or link to Other Source(s) used (e.g., sources not in checklist, templates) – Optional:

<http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>

<https://www.documents.dgs.ca.gov/sam/SamPrint/new/sam_master/sam_master_File/chap5300/5330.1.pdf> (SAM - 5330.1)