**Statewide Health Information Policy Manual (SHIPM) 3.1.4 – Security Management Process**

*Compliance Review Tool Question #43 (series)*

## Artifact Must Haves and Best Practices

| **Item #** | **Topic** | **Covered (Y or N)** | **Comment** |
| --- | --- | --- | --- |
| 1 | Did the organization submit an artifact(s) regarding how they perform Risk Assessments? |  |  |
| 2 | Does the artifact(s) describe the process/guidelines/methodology used to perform risk assessments, as follow: | n/a |  |
| 2a | * Identify the scope of the analysis?
 |  |  |
| 2b | * Identify the responsibility for the risk assessment, including appropriate participation of executive, technical and program management?
 |  |  |
| 2c | * Gather data?
 |  |  |
| 2d | * Identify and document potential threats and vulnerabilities (including probability and consequences)?
 |  |  |
| 2e | * Assess current security measures?
 |  |  |
| 2f | * Determine the likelihood of threat occurrence?
 |  |  |
| 2g | * Determine the potential impact of threat occurrence?
 |  |  |
| 2h | * Determine the level of risk?
 |  |  |
| 2i | * Identify security measures and finalize documentation?
 |  |  |
| 2j | * Identify and include risks related to Business Associates (*the BAs own risk assessments, and any findings of oversight*)?
 |  |  |
| 2k | * Include an approach to evaluating and understanding reported Incidents and Breaches (*including reviewing patterns, trends and mitigation strategies*)?
 |  |  |
| 3 | Does the artifact(s) identify the assets (system and facility) that are at risk? |  |  |
| 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? |  |  |
| 5 | Does the artifact(s) describe the process to address findings in the risk assessment in a timely manner? |  |  |
| 6 | Does the artifact(s) describe the process to monitor, track and address ongoing risk items and findings of the risk assessment? |  |  |
| 7 | Was the identified CAP (POAM) included as one of the documents submitted? |  |  |
| 8 | Are the items identified in the Risk Assessment being tracked and managed through a CAP (POAM)? |  |  |
| 9 | Does the artifact(s) describe how to communicate the results of the Risk Assessment to organization leadership? |  |  |
| 10 | Does the artifact(s) have official review/acceptance: | n/a |  |
| 10a | * Effective Date?
 |  |  |
| 10b | * Revision Date?
 |  |  |
| 10c | * Authorizing Senior/Executive Management Signature?
 |  |  |

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:

NIST [SP 800-30 Rev. 1 Guide for Conducting Risk Assessments publication](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final) can be found at the following link:

http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800\_30\_r1.pdf