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

*Compliance Review Tool Question #44 (series)*

## Artifact Must Haves

| **Item #** | **Topic** | **Covered (Y or N)** | **Comment** |
| --- | --- | --- | --- |
| 1 | Did the organization submit an artifact(s) requiring the protection of health information through the implementation of entity-wide risk management policies and procedures? | Y🞏 N🞏 |  |
| 2 | Is the artifact(s) current, published and authorized with contact information? | Y🞏 N🞏 |  |
| 3 | Does the artifact(s) describe the process/guidelines used to perform risk assessments? | Y🞏 N🞏 |  |
| 4 | Does the artifact(s) describe the methodology used to perform risk assessments? | Y🞏 N🞏 |  |
| 5 | Does the artifact(s) detail the requirements such as frequency, responsibility, and authorization used to complete the risk assessments? | Y🞏 N🞏 |  |
| 6 | Does the artifact(s) describe the process to address findings (e.g. POAM) in the risk assessment? | Y🞏 N🞏 |  |
| 7 | Does the artifact(s) describe how to communicate risk assessment results to key organizational personnel? | Y🞏 N🞏 |  |
| 8 | Does the artifact(s) describe the process to monitor and address ongoing risk items and findings of the risk assessment? | Y🞏 N🞏 |  |
| 9 | Does the artifact(s) clearly outline the requirements, such as timeframe (must be at least every 2 years), approach, priority, and impact needed to maintain the risk assessment? | Y🞏 N🞏 |  |
| 10 | Does the artifact(s) require the usage of malicious code protection mechanisms at all device entry/exits points on the network that detects and eradicates malicious code? |  |  |
| 11 | Does the artifact(s) have official review/acceptance: |  |  |
| 11a | * Effective Date?
 | Y🞏 N🞏 |  |
| 11b | * Revision Date?
 | Y🞏 N🞏 |  |
| 11c | * 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:

<https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=GOV&division=3.&title=2.&part=1.&chapter=5.7.&article=1>. (CA Government Code §11549.3)

<http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf>