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

*Compliance Review Tool Question #43 (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? |  |  |
| 2 | Is the artifact(s) current, published and authorized with contact information? |  |  |
| 3 | Does the artifact(s) describe the process/guidelines used to perform risk assessments? |  |  |
| 4 | Does the artifact(s) describe the methodology used to perform risk assessments? |  |  |
| 5 | Does the artifact(s) detail the requirements such as frequency, responsibility, and authorization used to complete the risk assessments? |  |  |
| 6 | Does the artifact(s) describe the process to address findings (e.g. POAM) in the risk assessment? |  |  |
| 7 | Does the artifact(s) describe how to communicate risk assessment results to key organizational personnel? |  |  |
| 8 | Does the artifact(s) describe the process to monitor and address ongoing risk items and findings of the risk assessment? |  |  |
| 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? |  |  |
| 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: | n/a |  |
| 11a | * Effective Date? |  |  |
| 11b | * Revision Date? |  |  |
| 11c | * Document the authorizing (senior or executive) management approval? |  |  |

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

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

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

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

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

Overall CDII Reviewer Comments:

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

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

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

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

Name of CDII 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](https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final) publication can be found at the following link:

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