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

*Compliance Review Tool Question #51*

## Artifact Must Haves

| **Item #** | **Topic** | **Covered (Y or N)** | **Comment** |
| --- | --- | --- | --- |
|  | Technical Security Evaluations |  |  |
| 1 | Did the organization submit an artifact(s) regarding how they perform technical Security Evaluations? |  |  |
| 2 | Does the artifact(s) describe the process/guidelines/methodology used to perform Technical Security Evaluations, as follow: | n/a |  |
| 2a | * Identify the scope of the analysis?
 |  |  |
| 2b | * Gather data?
 |  |  |
| 2c | * Identify and document potential threats and vulnerabilities (including probability and consequences)?
 |  |  |
| 2d | * Assess current security measures?
 |  |  |
| 2e | * Document the results of a vulnerability scan?
 |  |  |
| 2f | * Was the last vulnerability scan performed within the last two years?
 |  |  |
| 2g | * Determine the potential impact of identified vulnerabilities?
 |  |  |
| 2h | * Determine the level of risk?
 |  |  |
| 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 vulnerabilities in the Security Evaluation in a timely manner? |  |  |
| 6 | Does the artifact(s) describe how to communicate the results of the Security Evaluation to organization leadership? |  |  |
| 7 | Does the artifact(s) have official review/acceptance: | n/a |  |
| 7a | * Effective Date?
 |  |  |
| 7b | * Revision Date?
 |  |  |
| 7c | * Authorizing Sr. / Executive Management Signature?
 |  |  |
|  | Non-technical Security Evaluations |  |  |
| 8 | Did the organization submit an artifact(s) regarding how they perform non-technical Security Evaluations? |  |  |
| 9 | Does the artifact(s) describe the process/guidelines/methodology used to perform the non-technical Security Evaluations, as follow: | n/a |  |
| 9a | * Identify the scope of the analysis?
 |  |  |
| 9b | * Gather data?
 |  |  |
| 9c | * Identify and document potential threats and vulnerabilities (including probability and consequences)?
 |  |  |
| 9d | * Assess current security measures?
 |  |  |
| 9e | * Determine the potential impact of identified vulnerabilities?
 |  |  |
| 9f | * Determine the level of risk?
 |  |  |
| 10 | Does the artifact(s) identify the assets (system and facility) that are at risk? |  |  |
| 11 | 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? |  |  |
| 12 | Does the artifact(s) describe the process to address vulnerabilities in the Security Evaluation in a timely manner? |  |  |
| 13 | Does the artifact(s) describe how to communicate the results of the Security Evaluation to organization leadership? |  |  |
| 14 | Does the artifact(s) have official review/acceptance: | n/a |  |
| 14a | * Effective Date?
 |  |  |
| 14b | * Revision Date?
 |  |  |
| 14c | * 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 800-53 Assessing Security and Privacy Controls in Federal Information Systems and Organizations Building Effective Assessment Plans publication](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf) can be found at the following link:

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