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

*Compliance Review Tool Question #44 (series)*

## Artifact Must Haves and Best Practices

| **Item #** | **Topic** | **Covered (Y or N)** | **Comment** |
| --- | --- | --- | --- |
| 1 | Did the organization submit an artifact(s) that presents the results of an enterprise risk assessment / analysis (see NIST SP 800-30, Appendix K, Risk Assessment Reports – Essential Elements of Information)? |  |  |
| 2 | Does the artifact(s) describe the process/guidelines/methodology used to perform risk assessments, as follows: |  |  |
| 2a | * Does the artifact inform Tier 1 (Enterprise) decisions, as follows:
* Information security programs, policies, procedures and guidance?
* Risk responses (accept, avoid, mitigate, share or transfer)?
* Technology investment decisions?
* Entity-wide security controls?
* Enterprise/security architectures or monitoring strategies?
 |  |  |
| 2b | * Does the artifact inform Tier 2 (Business Process) decisions, as follows:
* Selection of common controls?
* Selection of suppliers, services, and contractors to support business functions?
* Application of information security policies to information systems and the environments in which they operate?
 |  |  |
| 2c | * Does the artifact inform Tier 3 (Information Asset) decisions, as follows:
* Selection and tailoring of security controls?
* Selection of technology products for information systems?
* Whether information technology products meet security control requirements?
* Operational decisions regarding the level of activity monitoring required and system maintenance approvals?
 |  |  |
| 3 | Does the artifact identify the scope of the analysis, including: |  |  |
| *The scope of the risk analysis (RA) is defined in terms of the entity to which it applies, how often it is performed, and the technologies to which it applies, all of which are driven by the business processes and underlying systems and/or technology that create, receive, maintain, or transmit Health Information in support of these business functions, and how often they and/or the underlying systems/technology/Health Information elements change.* |
| 3a | * Identify the responsibility for the risk assessment, including appropriate participation of executive, technical and program management?
 |  |  |
| 3b | * Is a comprehensive RA performed at least once every two years, or each time a significant change occurs in business programs/processes or supporting technology, or when Health Information elements are added or removed?
 |  |  |
| 3c | * Does the artifact address all of the entity’s Health Information, including the application systems, servers, databases, local and enterprise storage devices, workstations/mobile devices, printers and copiers, and wired/wireless transmission media, regardless of the electronic medium in which it is created, received, maintained or transmitted?
 |  |  |
| 3d | * Does the artifact address all of the entity’s Health Information, regardless of location, including both covered entity and business associate locations, such as local/remote business processing centers, on-premises technical infrastructure, and off-premises/hybrid technical infrastructure, fully or partially hosted by cloud service providers (CSPs)?
 |  |  |
| 4 | Does the artifact(s) include assumptions and constraints, as follows: |  |  |
| Key assumptions relevant to the risk assessment can include:* Assessment and analysis approaches used
* Business functions using Health Information

Key constraints relevant to the risk assessment can include:* Resources available for the assessment
* Skills/expertise required for the assessment
* Operational considerations (e.g., the use of best- or worst-case projections in assessing threats and impacts)

The HIPAA Security Rule requirement for Risk Analysis is to “*Conduct an* ***accurate*** *and* ***thorough*** *assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”* Because of this, the above items should be considered in their broadest context for the purposes of this Risk Assessment.  |
| 4a | * Does the artifact identify the specific assumptions under which the risk assessment is conducted?
 |  |  |
| 4b | * Does the artifact identify the specific constraints under which the risk assessment is conducted?
 |  |  |
| 5 | Does the artifact(s) include sources of * descriptive,
* threat,
* vulnerability,
* and impact information, as follows:
 |  |  |
| ***Descriptive*** *- this information helps entities determine the relevance of threat and vulnerability information. Types and sources of information applicable to each Tier are described below:**Tier 1 – Risk management and information security governance structures, and Business Impact Assessments (BIAs) often indicate how entities identify and prioritize critical business functions (in this case, those that work with Health Information).**Tier 2 – Business Continuity plans, Risk Assessment reports, and Business Associate Agreements (BAAs) are good sources of information re: operations and management processes, technical and information flows, business architecture, security architecture, common infrastructures, shared services, external relationships and dependencies upon service providers.**Tier 3 – System documentation, contingency plans, and risk assessment reports for other information systems, infrastructures, and services often provide information re: designs and technologies used in entity information systems, the environment in which they operate, connectivity to and dependency on other information systems, common infrastructures or shared services.****Threat*** *– see the tables in Appendixes D and E of the NIST SP 800-30 r1 Guide for Conducting Risk Assessments. Sources of vulnerability information can be either internal or external (see Table E-1). Internal sources can include incident/breach logs/reports. External sources can be open source and/or proprietary threat reports, and previous risk/threat assessments.****Vulnerabilities*** *– see the tables in Appendix F of the NIST SP 800-30 r1 Guide for Conducting Risk Assessments. Sources of vulnerability information can be either internal or external (see Table F-1). Internal sources can include vulnerability assessment reports and incident/breach logs/reports. External sources are similar to the sources identified above for threat information.****Impact*** *– Tables in Appendix H (of the NIST SP 800-30 r1 Guide for Conducting Risk Assessments) list examples of adverse impacts and scales for the level of impact.* |
| 5a | * Which of the following artifacts were submitted:
* Risk Analysis/Assessment?
* Security Evaluations
	+ Technical (e.g., CA DoM)
		- Vulnerability Scans?
		- Penetration Tests?
	+ Non-Technical (i.e., physical & administrative)
		- Legal?
		- Policy & procedure review?
		- Training review?
* Business Impact Analysis (BIA)?
* Business Continuity Plan (BCP)?
* Technology Recovery Plan (TRP)?
 |  |  |
| 5b | * Does the artifact identify the sources of threat information (see the tables in Appendix D of NIST SP 800-30 r1 for examples)?
 |  |  |
| 5c | * Does the artifact identify the sources of vulnerability information (see the tables in Appendix F of NIST SP 800-30 r1 for examples)?
 |  |  |
| 5d | * Does the artifact identify the sources of impact information (see the tables in Appendix H of NIST SP 800-30 r1 for examples)?
 |  |  |
| 6 | Does the artifact describe the Risk Model and Analytic Approach, as follows: |  |  |
| *This is how the assessment process works. The Risk Model defines key terms and assessable risk factors, such as threats, threat sources, and threat events, vulnerabilities, and the relationships among the factors.**The Analytic Approach describes how the risk factors are analyzed in order to determine risk. Analysis approaches differ with respect to the starting point of the risk assessment, level of detail in the assessment, and how risks due to similar threat scenarios are treated.**The Analytic Approach can be: threat-oriented; asset/impact-oriented; or vulnerability-oriented. A threat-oriented approach first identifies threat sources and threat events, then focuses on the development of threat scenarios; vulnerabilities are identified in the context of threats, and for adversarial threats, impacts are identified based on adversary intent. An asset/impact-oriented approach first identifies impacts and critical assets, possibly using the results of a business impact analysis (BIA) then identifies threat events that could lead to and/or threat sources that could seek those impacts. A vulnerability-oriented approach starts with a set of exploitable weaknesses in information systems or the operating environments, and identifies threat events that could exploit the vulnerabilities along with possible impacts. Each approach uses the same risk factors and assessment activities, just in a different order.*[NOTE: NIST SP 800-34 provides guidance on BIAs at the information system level of the risk management hierarchy.] |
| 6a | * Does the artifact describe risk factors in qualitative (low, moderate, or high), quantitative (10, 20, 30, etc.), or semi-quantitative (0-15, 16-35, 36-70…) terms and provide their associated values?
 |  |  |
| 6b | * Does the artifact describe the relationship between the risk factors and how they are used to determine risk?
 |  |  |
| 7 | Does the artifact include the assignment of responsibilities for Risk Assessment, as follows: |  |  |
| 7a | * Does the artifact clearly identify how executive management participates in the risk assessment and who is responsible for what?
 |  |  |
| 7b | * Does the artifact clearly identify how technical management participates in the risk assessment and who is responsible for what?
 |  |  |
| 7c | * Does the artifact clearly identify how program management participates in the risk assessment and who is responsible for what?
 |  |  |
| 8 | Does the artifact include information regarding data collection, as follows: |  |  |
| *An entity must identify where the Health Information is stored, received, maintained or transmitted. An entity could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on Health Information gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)* |
| 8a | * Does the artifact contain application system flow diagrams for all state entity systems that create, receive, maintain, or transmit Health Information?
 |  |   |
| 8b | * Does the artifact contain network diagrams that show the technology components (e.g., web, application, and database servers, local and enterprise storage, local, remote, and mobile end user devices) for systems that create, receive, maintain, or transmit Health Information?
 |  |  |
| 8c | * Does the artifact identify all operating environments that create, receive, maintain, or transmit production Health Information, including production failover/fallback, backup/replication, or other environments, regardless of physical location?
 |  |  |
| 8d | * Does the artifact identify all non-production operating environments that create, receive, maintain, or transmit production Health Information, including development, test, quality assurance, staging, or others, if applicable?
 |  |  |
| 9 | Does the artifact identify and document potential threats, as follows: |  |  |
| *Entities must identify and document reasonably anticipated threats to Health Information (45 C.F.R. §§ 164.306(a)(2) and 164.316(b)(1)(ii)). This includes the identification of potential threat events, relevance of the events, and the threat sources that could initiate the events. In addition, consideration should be given to potential threats across all Tiers:****Tier 1*** *– Enterprise: threats related to organizational enterprise governance, external business relationships, including HIPAA Business Associates (BAs), management/operational policies, procedures, and structures.* ***Tier 2*** *– Business Process: threats related to business processes, support services, common infrastructure and common controls, including HIPAA Business Associates (BAs) and the Health Information to which they have access.****Tier 3*** *– Information asset: threats related to application systems, information technologies, system components, networks and operating environments, including HIPAA Business Associates (BAs), their information assets, and the Health Information to which they have access.**The tables contained in Appendixes D and E of NIST SP 800-30 r1 provide examples of the above information for both adversarial and non-adversarial threats, and other relevant information.* |
| 9a | * Does the artifact contain all reasonably anticipated threats to systems that create, receive, maintain, or transmit Health Information, including premises-based, cloud-based, and hybrid operating environments, as applicable?
 |  |  |
| 9b | * Which of the following artifacts were submitted:
* Risk Analysis/Assessment?
* Security Evaluations
	+ Technical (e.g., CA DoM)
		- Vulnerability Scans?
		- Penetration Tests?
	+ Non-Technical (i.e., physical & administrative)
		- Legal?
		- Policy & procedure review?
		- Training review?
* Business Impact Analysis (BIA)?
* Business Continuity Plan (BCP)?
* Technology Recovery Plan (TRP)?
 |  |  |
| 9c | * Does the artifact address BAs and the Health Information to which they have access?
 |  |  |
| 9d | * Does the artifact address threats across all Tiers?
 |  |  |
| 9e | * Does the artifact address the following threat types:
* Adversarial?
* Accidental?
* Structural (IT hardware, software, environmental)?
* Natural/man-made disasters, infrastructure outages?
 |  |  |
| 10 | Does the artifact identify and document potential vulnerabilities, including: |  |  |
| *Entities must identify and document vulnerabilities which, if triggered or exploited by a threat, would create* ***a risk of inappropriate access to or disclosure of Health Information*** *(45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii)).**In addition, consideration should be given to vulnerabilities across all Tiers:****Tier 1*** *– Enterprise: vulnerabilities related to enterprise governance, external business relationships, including BAs, management/operational policies, procedures, and structures.****Tier 2*** *– Business Process: vulnerabilities related to business processes, support services, common infrastructure, and common controls, including BAs and the Health Information to which they have access.****Tier 3*** *– Information asset: vulnerabilities related to application systems, information technologies, system components, networks, and operating environments, including BAs and the Health Information to which they have access.**The tables contained in Appendix F of NIST SP 800-30 r1 provide information regarding vulnerabilities across all Tiers and assessment of severity.* |
| 10a | * Does the artifact contain vulnerabilities?
 |  |  |
| 10b | * Which of the following artifacts were submitted:
* Risk Analysis/Assessment?
* Security Evaluations
	+ Technical (e.g., CA DoM)
		- Vulnerability Scans?
		- Penetration Tests?
	+ Non-technical (i.e., physical & administrative)
		- Legal?
		- Policy & procedure review?
		- Training review?
* Business Impact Analysis (BIA)?
* Business Continuity Plan (BCP)?
* Technology Recovery Plan (TRP)?
 |  |  |
| 10c | Does the artifact address BAs and the Health Information to which they have access? |  |  |
| 10d | Does the artifact address vulnerabilities across all Tiers? |  |  |
| 11 | Does the artifact assess current security measures, including: |  |  |
| *State entities should assess and document the security measures used to safeguard Health Information, to determine whether the security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1)).* |
| 11a | * Was an assessment performed of the current security measures used to safeguard Health Information in order to confirm that the required controls are implemented, configured, and functioning properly?
 |  |  |
| 11b | * Did the assessment include both technical and non-technical (physical and administrative) controls within its scope?
 |  |  |
| 11c | * Was the Plan of Action and Milestones (POAM) produced for use in reporting and managing findings?
 |  |   |
| 12 | Does the artifact determine the likelihood of threat event occurrence, including: |  |  |
| *The Security Rule requires entities to take into account the probability of potential risks to Health Information. (45 C.F.R. § 164.306(b)(2)(iv)). The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires protection against because they are “reasonably anticipated.”****The output of this part should be documentation of all threat and vulnerability combinations with associated likelihood estimates*** *that may impact the confidentiality, availability and integrity of Health Information of an entity. (45 C.F.R. §§ 164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii)).**In addition, consideration should be given to the determination of the likelihood of reasonably anticipated threats across all Tiers:****Tier 1*** *– Enterprise: likelihood related to enterprise governance, external business relationships, management/operational policies, procedures, and structures.****Tier 2*** *– Business Process: likelihood related to business processes, support services, common infrastructure and common controls.****Tier 3*** *– Information asset: likelihood related to application systems, information technologies, system components, networks, and operating environments.**The tables contained in Appendix G of NIST SP 800-30 r1 provide an assessment scale for Tier 1 and additional inputs for Tier 3, if needed.* |
| 12a | * Does the artifact contain a list of threat and vulnerability combinations with the likelihood of occurrence identified for each?
 |  |  |
| 12b | * Did the list include items associated with all Tiers?
 |  |  |
| 13 | Does the artifact determine the potential harm of threat occurrence, including: |  |  |
| *The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of Health Information. (45 C.F.R. § 164.306(b)(2)(iv)). The entity must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. The method can be qualitative (low, moderate, or high, quantitative (10, 20, 30, etc.), or semi-quantitative (0-15, 16-35, 36-70…).****The output of this process should be a list of all potential impacts*** *associated with the occurrence of reasonably anticipated threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of Health Information within an entity. (45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii)).**In addition, consideration should be given to the determination of the impact of reasonably anticipated threats across all Tiers:****Tier 1*** *– Enterprise: impact related to enterprise governance, external business relationships, management/operational policies, procedures, and structures.****Tier 2*** *– Business Process: impact related to business processes, support services, common infrastructure and common controls.****Tier 3*** *– Information asset: impact related to application systems, information technologies, system components, networks and operating environments.**The tables contained in Appendix H of NIST SP 800-30 r1 provide examples of adverse impacts (harm), an assessment scale for Tier 1 and additional inputs for Tiers 2 and 3, if needed.* |
| 13a | * Does the artifact identify and document the adverse impacts (harm) of a reasonably anticipated threat that affects the confidentiality, availability, and integrity of Health Information within the entity?
 |  |  |
| 13b | * Does the artifact address the adverse impacts (harm) of reasonably anticipated threats across all Tiers?
 |  |  |
| 14 | Does the artifact determine the level of risk and cost of mitigation, including: |  |  |
| *Entities should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. A common method of calculating risk levels is to adjust the impact value based on the likelihood/probability of the occurrence of the threat event. For example, if the estimated impact (harm) of a ransomware attack is $500,000 based on ransom paid, revenue lost and resources used for remediation and recovery, and the probability of a successful phishing attack and subsequent malware installation and execution is 20%, the risk in dollars is: $500,000 x 20% = $100,000. Of course this is for a quantitative approach to Risk Estimation. A qualitative approach would be defined differently and both are acceptable as long as they adjust impact for probability.**The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level (45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)).* |
| 14a | * Does the artifact identify the risk level for all threat and vulnerability combinations identified during the risk analysis?
 |  |   |
| 14b | * Does the artifact identify cost-effective controls to be implemented in order to reduce the risk for each threat/vulnerability combination to an acceptable level, or indicate acceptance of the risk outright?
 |  |   |
| 15 | Does the artifact include risk analysis / assessment documentation, including: |  |  |
| *Entities should prepare a report to be submitted to the state entity’s enterprise governance organization and/or entity head and other entities in accordance with SAM, and to be kept on file within the state entity, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of residual risk to be accepted by the state entity. Findings that require mitigation/remediation should be presented along with the report and managed using the Plan of Action and Milestones (POAM).* |
| 15a | * Does the artifact report all elements described in this document as requested and submitted through the review (i.e., compliance review, focused review) request process?
 |  |  |
| 15b | * Was the artifact submitted to the state entity’s governance organization and / or entity head and other entities in accordance with SAM, and kept on file within the state entity, as evidenced by their policies and procedures?
 |  |  |
| 15c | * Did the artifact document the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of residual risk to be accepted by the state entity?
 |  |  |
| 15d | * Was a POAM prepared and submitted to the appropriate entities along with the Risk Analysis Report, in accordance with the state entity’s policies and procedures and the following:
* SAM 5305.1 – Information Security Program Management?
* SIMM 5305 – Plan of Action and Milestones FAQs?
* SIMM 5305-B – Plan of Action and Milestones Instructions?
* SIMM 5305-C – Plan of Actions and Milestones worksheet?
 |  |  |
| 16 | Does the artifact include Risk Analysis / Assessment Monitoring and Maintenance information, including: |  |  |
| *Conduct continuous monitoring of the risk factors (threats and vulnerabilities, incidents and breaches), new sub-entities, significant changes in business processes and/or the supporting systems in which Health Information is created, received, maintained, or transmitted, that contribute to changes in the associated risk. Update the Risk Assessment more frequently than bi-annually, based on any significant organizational, process or technical changes.* |
| 16a | * Does the artifact require the continuous monitoring and reporting of risk factors associated with new sub-entities, significant changes in business processes and/or the supporting systems that create, receive, maintain, or transmit Health Information?
 |  |  |
| 16b | * Does the artifact contain language that requires updates to the Risk Assessment based on the results of continuous monitoring and reporting of risk factors?
 |  |  |
| 16c | * Does the artifact contain language that requires updates to the POAM based on the results of continuous monitoring and reporting of risk factors?
 |  |  |
| 17 | Does the artifact(s) describe how to communicate the results of the Risk Assessment to organization leadership? |  |  |
| 18 | Does the artifact(s) have official review/acceptance: |  |  |
| 18a | * Effective Date?
 |  |  |
| 18b | * Revision Date?
 |  |  |
| 18c | * 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:

<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>