

## RISK ASSESSMENT Reference Chart

TOPIC & REFERENCE	* SAM	* NIST 800-53	* HIPAA
Risk Assessment			
Risk Assessment Policy & Procedures	5305-5305.2 and 5355.3 Risk management is the process of taking actions to avoid or reduce risk to acceptable levels. This process includes both the identification and assessment of risk through risk analysis (SAM Section 5305.1) and the initiation and monitoring of appropriate practices in response to that analysis through the agency's risk management program. Policy and procedures should address these issues.	<p>RA-1 The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance, and (ii) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.</p> <p>NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>	164.308(a)(1) (CalOHI Policy Memorandum <a href="#">2004-43</a> , <a href="#">2005-54</a> and <a href="#">2005-55</a> .) Security management process standard of the Security Rule requires that covered entities implement policies and procedures to prevent, detect, contain, and correct security violations. The risk analysis, risk management, sanction policy, and information system activity review requirements are to be used to accomplish this.
Security Categorization	5320.5 Classification of Information Automated files and databases are an essential public resource that must be give appropriate protection from loss, inappropriate disclosure, and unauthorized modification. Refer to Section 5320.5 for current classification structures.	<p>RA-2 The organization categorizes the information system and the information processed, stored, or transmitted by the system in accordance with FIPS 199 and documents the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organization review and approve the security categorizations.</p> <p>The organization conducts security categorizations as an organization-wide activity with the involvement of the chief information officer, senior agency information officer, information system owners, and information owners.</p>	While not required or addressable in HIPAA, CalOHI Policy Memorandum <a href="#">2005-62</a> , Contingency Plan addresses the need to classify and categorize data so that proper precautions can be taken for different classifications of data.

\*Description of the topic items are a summary or excerpt from the actual policy. Agencies should refer to the specific policy instrument for actual language.

## RISK ASSESSMENT Reference Chart

TOPIC & REFERENCE	* SAM	* NIST 800-53	* HIPAA
		NIST Special Publication 800-60 provides guidance on determining the security categories of the information types resident on the information system.	
Risk Assessment	5305.1 A risk analysis process identifies and assesses risks associated with information assets and defines a cost-effective approach to managing such risks. Specific risks that must be addressed include, but are not limited to, those associated with accidental and deliberate acts on the part of an agency employees and outsiders; fire, flooding, and electric disturbances; and loss of data communications capabilities.	<p>RA-3 The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the information system.</p> <p>NIST Special Publication 800-30 provides guidance on conducting risk assessments including threat, vulnerability, and impact assessments.</p>	164.308(a)(1) (CalOHI Policy Memorandum <a href="#">2004-43</a> , <a href="#">2005-54</a> and <a href="#">2005-55</a> .) Effective risk management cannot be performed without the risk analysis, which identifies vulnerabilities to threats and their impact. The risk management must be performed on an ongoing basis; not just once. Implementing a continuous cycle of well-organized risk management activities is the key to ensuring adequate consideration of the changing information security risks and resources.
Vulnerability scanning	<p>5310 Establishing appropriate department policies and procedures to protect and secure IT infrastructure, including:</p> <ul style="list-style-type: none"> <li>▪ Technology upgrades</li> <li>▪ Security patches and security upgrades</li> <li>▪ Firewall configurations</li> <li>▪ Server hardening and configuration</li> </ul>	<p>RA-5 Using appropriate vulnerability scanning tools and techniques, the organization scans for vulnerabilities in the information systems or when significant new vulnerabilities affecting the system are identified and reported.</p> <p>The organization trains selected</p>	While not required or addressable by HIPAA, vulnerability scanning should be a part of organization's security management process. CalOHI Policy Memorandum <a href="#">2005-56</a> Security Management Vulnerability assessments consists of covered entities performing

\*Description of the topic items are a summary or excerpt from the actual policy. Agencies should refer to the specific policy instrument for actual language.

## RISK ASSESSMENT Reference Chart

TOPIC & REFERENCE	* SAM	* NIST 800-53	* HIPAA
	<ul style="list-style-type: none"> <li>▪ Software management and licensing</li> <li>▪ Prohibition of technology for any non-business purpose</li> </ul>	<p>personnel in the use and maintenance of vulnerability scanning tools and techniques. The information obtained from the vulnerability scanning process is freely shared with appropriate personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.</p> <p>NIST Special Publication 800-40 provides guidance on handling security patches.</p>	<p>technical and non-technical assessments of their computing environments, where EPHI is accessed, stored, transmitted, or received. Vulnerabilities are flaws or weaknesses in system security procedures, designs, and implementation or internal controls that could result in a security breach or a violation of the system's security policy. The assessments should identify current controls and system vulnerabilities to threats.</p>
Awareness and Training			
Security Awareness and Training Policy & Procedures	<p>5325 Personnel Practices. Personnel practices related to security management must include training of agency employees with respect to individual, agency, and statewide security responsibilities and policies. Agencies should contact the Department of Personnel Administration for specific rules.</p>	<p>AT-1 The organization develops, disseminates, and periodically reviews/updates: (I) a formal, documented, security awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls.</p> <p>The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general, and for a particular information system, when</p>	<p>164.308(a)(5) Implement a security awareness and training program for all members of its workforce (including management). ) (CalOHI Policy Memorandum <a href="#">2004-57</a> Security Awareness and Training)</p>

\*Description of the topic items are a summary or excerpt from the actual policy. Agencies should refer to the specific policy instrument for actual language.

## RISK ASSESSMENT Reference Chart

TOPIC & REFERENCE	* SAM	* NIST 800-53	* HIPAA
		<p>required.</p> <p>NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>	
Security Awareness	5325 Personnel Practices related to security management must include training of agency employees with respect to individual, agency, and statewide security responsibilities.	<p>AT-2 The organization ensures all users (including managers and senior executive) are exposed to basic information system security awareness materials before authorizing access to the system and thereafter.</p> <p>The organization determines the appropriate content of security awareness training based on the specific requirements of the organization and the information systems to which personnel have authorized access. The organization's security awareness program is consistent with the requirements contained in 5 C.F.R. Part 930-301 and with the guidance in NIST Special Publication 800-50.</p>	<p>164.308(a)(5)(i) implement a security awareness training program for all members of its workforce (including management). (CalOHI Policy Memorandum <a href="#">2004-57</a> Security Awareness and Training)</p> <p>(ii) Implementation specifications. Implement: Security reminders. Periodic security updates. Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software. Log-in monitoring. Procedures for monitoring log-in attempts and reporting discrepancies. Password management. Procedures for creating, changing, and safeguarding passwords.</p>
Personnel Security			
Personnel Security Policy and Procedures	5325 Agency Risk Management Program.	<p>PS-1 The organization develops, disseminates, and periodically reviews/updates: (I) formal, documented, personnel security policy that addresses purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate</p>	<p>164.308(a)(3) (i) <i>Standard: Workforce security.</i> (CalOHI Policy Memorandum <a href="#">2005-69</a> Workforce Security) Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as</p>

\*Description of the topic items are a summary or excerpt from the actual policy. Agencies should refer to the specific policy instrument for actual language.

## RISK ASSESSMENT Reference Chart

TOPIC & REFERENCE	* SAM	* NIST 800-53	* HIPAA
		<p>the implementation of the personnel security policy and associated personnel security controls.</p> <p>The personnel security policy can be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general, and for a particular information system, when required.</p> <p>NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>	<p>provided under Paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.</p>
Position Categorization	<p>Personnel roles and responsibilities</p> <p>5315.1 Agency Management Responsibilities</p> <p>5320.2 Responsibility of owners of information</p> <p>5320.3 Responsibilities of custodians of information</p> <p>5320.4 Responsibility of users of information</p>	<p>PS-2 The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations.</p> <p>The risk designations are consistent with 5 CFR 731.106a) and Office of Personnel Management policy and guidance.</p>	<p>164.308(a)(3) (A) <i>Authorization and/or supervision</i> (CalOHI Policy Memorandum <a href="#">2005-68</a>, Access Administration) Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.</p>
Personnel Termination	<p>5325 Personnel Practices</p> <p>Termination procedures ensure that agency information assets are not accessible to former employees.</p>	<p>PS-4 When employment is terminated, the organization terminates information system access, conducts exit interviews, ensures the return of all organizational information system-related property (e.g., keys, identification cards, building passes),</p>	<p>164.308(a)(3) (C) <i>Termination procedures</i> (CalOHI Policy Memorandum <a href="#">2005-69</a> Workforce Security) Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or required by</p>

\*Description of the topic items are a summary or excerpt from the actual policy. Agencies should refer to the specific policy instrument for actual language.

## RISK ASSESSMENT Reference Chart

TOPIC & REFERENCE	* SAM	* NIST 800-53	* HIPAA
		and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organizational information systems.	paragraph (a)(3)(ii)(B) of this section.
Third-Party Personnel Security	5335.1 – Information Integrity and Security  Agreements with non-state entities	PS-7 The organization establishes personnel security requirements for third-party providers (e.g., service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, network and security management) and monitors provider compliance to ensure adequate security.  The organization explicitly includes personnel security requirements in acquisition-related documents.  NIST Special Pub 800-35 provides guidance on information technology security services.	164.308(b)(1) <i>Standard: Business associate contracts and other arrangements.</i> (CalOHI Policy Memorandum <a href="#">2002-15</a> Business Associate Templates) A covered entity, in accordance with § 164.306, may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.
Personnel Screening	5325 Personnel Practices Employment history and/or background checks on employees who work with or have access to confidential or sensitive information or critical applications.	PS-3 The organization screens individuals requiring access to organization information and information systems before authorizing access.  Screening is consistent with: (I) 5 CFR 731.106(a); (ii) Office of Personnel Management Policy, regulations, and guidance; (iii) organizational policy, regulations,	164.308(a)(3) (B) <i>Workforce clearance procedure</i> (CalOHI Policy Memorandum <a href="#">2005-69</a> Workforce Security) Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.

\*Description of the topic items are a summary or excerpt from the actual policy. Agencies should refer to the specific policy instrument for actual language.

## RISK ASSESSMENT Reference Chart

TOPIC & REFERENCE	* SAM	* NIST 800-53	* HIPAA
		and guidance; (iv) FIPS 201 and Special Publication 800-73 and 800-76; and (v) the criteria established for the risk designation of the assigned positions.	
Physical and Environmental Protection			
Physical and Environmental Protection Policy and Procedures	5330 Agency physical security measures must provide for management control of physical access to information assets (including personnel computer systems and computer terminals) by agency staff and outsiders; prevention, detection, and suppression of fires; prevention, detection, and minimization of water damage; and protection, detection, and minimization of loss or disruption of operational capabilities due to electrical power fluctuations or failure.	<p>PE-1 The organization develops, disseminates, and periodically reviews-updates: (I) a formal, documented, physical and environmental protection policy that address purpose, scope, roles, responsibilities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.</p> <p>The physical and environmental protection policy can be included as part of the general information security policy for the organization. Physical and environmental protection procedures can be developed for the security program in general, and for a particular information system, when required. NIST Special Publication 800-12 provides guidance on security policies and procedures.</p>	164.310(a)(1) (CalOHI Policy Memorandum <a href="#">2005-63</a> Facility Access Controls) Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
Physical Access Authorizations	5340 Physical security practices for each facility must be adequate to protect the	PE-2 The organization develops and keeps current lists of personnel with	164.310(a)(1) (CalOHI Policy Memorandum <a href="#">2005-63</a> Facility

\*Description of the topic items are a summary or excerpt from the actual policy. Agencies should refer to the specific policy instrument for actual language.

## RISK ASSESSMENT Reference Chart

TOPIC & REFERENCE	* SAM	* NIST 800-53	* HIPAA
	most sensitive information technology application housed in that facility.	<p>authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials.</p> <p>The organization promptly removes personnel no longer requiring access from access lists.</p>	Access Controls) Facility Security Plan (Addressable). Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
Monitoring Physical Access	<p>5305.2 – Agency Risk Management Program</p> <p>Physical security practices - Agency physical security measures must provide for management control of physical access to information assets. Physical security practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility</p>	<p>PE-6 The organization monitors physical access to information systems to detect and respond to incidents.</p> <p>The organization review physical access logs periodically, investigates apparent security violations or suspicious physical access activities, and takes remedial actions.</p>	164.310(a)(1) (CalOHI Policy Memorandum <a href="#">2005-63</a> Facility Access Controls) Maintenance records, need-to-know procedures for personnel access, sign-in for visitors and escort, if appropriate, and testing and revision. Maintenance Records (Addressable). Implement policies and procedures to document repairs and modification to the physical components of a facility which are related to security...”
Physical Access Controls	<p>5305.2 – Agency Risk Management Program</p> <p>Physical security practices - Agency physical security measures must provide for management control of physical access to information assets. Physical security</p>	PE-3 The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible)	164.310(a)(1) (CalOHI Policy Memorandum <a href="#">2005-63</a> Facility Access Controls) Controls would include the following implementation features: disaster recovery, emergency mode operation, equipment control (into

\*Description of the topic items are a summary or excerpt from the actual policy. Agencies should refer to the specific policy instrument for actual language.

## RISK ASSESSMENT Reference Chart

TOPIC & REFERENCE	* SAM	* NIST 800-53	* HIPAA
	<p>practices for each facility must be adequate to protect the most sensitive information technology application housed in that facility</p>	<p>and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.</p> <p>The organization uses physical access devices (e.g., keys, locks, combinations, card readers) and/or guards to control entry to facilities containing information systems. The organization secures keys, combinations, and other access devices and inventories those devices regularly. The organization changes combinations and keys: (I) periodically; and (ii) when keys are lost, combinations are compromised, or individuals are transferred or terminated. After an emergency-related event, the organization restricts reentry to facilities to authorized individuals only. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being appropriately controlled.</p>	<p>and out of site).</p>

\*Description of the topic items are a summary or excerpt from the actual policy. Agencies should refer to the specific policy instrument for actual language.