DHHS Information Technology (IT) Risk Management Standard

Issue Date: October 1, 2013
Effective Date: October 1, 2013
Revised Date:

Number: DHHS-2013-001-C

1.0 Purpose and Objectives

Protecting and ensuring the Confidentiality, Integrity, and Availability (CIA) for all Nebraska Department of Health and Human Services (DHHS) information and information systems is a fundamental objective of the DHHS Information Security. The DHHS Information Technology Risk Management Standards is a critical component of ensuring that all DHHS information is protected appropriately. The purpose of this standard is to describe the detailed requirements and procedures to be followed throughout the DHHS infrastructure to ensure that all information owned, controlled, or managed by DHHS is protected commensurate with its information classification, and that business areas are in compliance with DHHS policies and standards. The DHHS Information Security Officer (ISO) is required to perform periodic reviews, inspections, and assessments of the security posture in place throughout DHHS. This standard describes the reviews that are required to be conducted, and the format in which these reviews will take place.

2.0 Scope and Applicability

It is DHHS Policy that scheduled and random risk assessments will be conducted on DHHS IT resources maintaining or accessing DHHS information. All business areas of DHHS that process or handle non-public information are subject to review and inspection following these standards. All physical locations and information technology supporting DHHS services are subject to these reviews. Business and IS&T Management are required to work with the ISO to establish schedules for the reviews as requested, to accommodate business schedules within reason, and to make available all personnel, information, physical areas, records, and historical documentation to facilitate these reviews. The ISO is required to establish schedules and priorities based upon known or likely levels of security risks to DHHS information or services.

2.1 Enforcement

Violation of this standard, as it includes compliance with federal and state regulations, may result in criminal and monetary penalties for individuals found violating these standards. Any staff member found to have violated this policy may be subject to disciplinary action, as defined in the governing policy DHHS-2013-001 *DHHS IT Security Policy*.

3.0 Standard

DHHS is required to implement policies, standards, and procedures to prevent, detect, contain, and correct security deficiencies. Furthermore, DHHS is required to implement risk analysis and risk management to ensure adequate resources, policies, procedures, processes, and practices are in place and compliant with DHHS standards and procedures.

Risk management is an essential function that is a perpetual focus within the DHHS systems development practice. In order to have effective risk management, Information Systems and Technology (IS&T) and the ISO are required to plan for the use of technology, assess the risk associated with technology, decide how to securely implement the technology, and establish a process to measure and monitor risk.

The key elements of the DHHS Risk Management Program include:

I. Operational Planning: Operational planning shall identify and assess risk exposure to ensure policies, procedures, and controls remain effective. Risk reviews and assessments should address the Confidentiality, Integrity, and Availability (CIA) of the systems, controls, and foreseeable internal and external threats. DHHS business owners need to consider the results of assessments when overseeing operations.

II. Ongoing Data Collection: Understanding of the systems environment is critical to an effective risk management program. There are several sources of information that can provide valuable input into the DHHS Risk Management Program. The ISO shall validate and review:

   a. IS&T Strategic and Tactical Plans
   b. Disaster Recovery and Business Continuity Plans
   c. IS&T Help Desk tickets and tracking reports
   d. Self-assessments on security controls
   e. Reported security incidents

III. Risk Analysis: DHHS business owners and the ISO shall use information collected on IT assets and risks to analyze the potential impact of risks on the system and business functions. The analysis should identify various events or threats that could negatively affect the system strategically or operationally. The ISO shall evaluate the likelihood of various events and rank the possible impact.

IV. Inspection and Monitoring: The ISO shall perform reviews and inspections of DHHS systems and business processes. ISO and impacted business owners shall monitor risk mitigation activities to ensure appropriate progress is being made on risk mitigation or remediation. This monitoring shall be recorded in the DHHS Plan of Action and Milestones (POA&M) process.

Risk assessments and reviews will evaluate the potential security risk a defined IT resource's vulnerabilities may have and their potential impact it may have on other DHHS IT resources. The risk assessments will be a joint venture between IS&T and the DHHS division, department, or program area accountable for the IT resource included in a risk assessment. DHHS has established three levels of scheduled reviews with an intention of addressing risk from three perspectives:

I. Business Process Review - reviewing risk from the individual business perspective
II. HIPAA Focus - reviewing risk from the information (PHI) perspective
III. Federal Information Security Management (FISMA) Review - reviewing risk from the infrastructure and organization perspective

3.1 Business Process Risk Assessment

The intent of the Business Process Risk Assessment is to validate that individual departments across DHHS are in compliance with *DHHS-2013-001 DHHS IT Security Policy*, particularly where the highest level of risks exist to DHHS information. This review is focused specifically on the individual business process, and includes a review of all information input, processing, and output from the business process. It will review all touch points, exposure points, and information flow to ensure the information is protected commensurate with its classification throughout the business process.

Because of the large volume of business processes throughout DHHS, and the various levels of information handled by these departments, it is not practical to review all business areas on a regular basis. In fact, it is more likely that higher-risk business processes may be reviewed multiple times before lower-risk processes are reviewed. The ISO shall prepare an annual schedule of Business Process reviews, with input from the DHHS Privacy Officer and other DHHS and IS&T management. These reviews shall occur at least four (4) times per year (quarterly), and all findings shall be recorded and tracked in the POA&M process. The schedule of reviews shall be based on priorities that are determined using the following considerations:

a. Classification level of the information used within the business process
b. Evaluation of key risk indicators and their related factors
c. Evaluation of threats that are imminent or unique to the business process
d. Past performance, previous incidents or exposures, past audit or review findings
e. Impact analysis to DHHS of a security breach within the business process
f. Management discretion, concerns, or advice

3.2 HIPAA Risk Assessment

It is DHHS policy that all DHHS divisions, departments, and program areas (hereinafter referred to as "PHI Owner") who use, create, process, receive, transmit, or store electronic Protected Health Information (PHI) will maintain a current Health Insurance Portability and

Accountability Act (HIPAA) Risk Assessment for the handling and protection of PHI. The intent of this review is to focus primarily on the areas of DHHS that are handling PHI and to ensure that all PHI is secured with an appropriate level of administrative, physical, and technical safeguards - per the "Security Standards for the Protection of Electronic Protected Health Information (EPHI)" found at 45 CFR Part 164, Subpart C, commonly known as the Security Rule.

The ISO serving as the DHHS HIPAA Security Officer will be responsible for scheduling and managing HIPAA Risk Assessments. HIPAA Risk Assessments will be a joint venture between the HIPAA Security Officer and the PHI Owner.

HIPAA Risk Assessments will be conducted:

- At minimum, once every five (5) years
- When significant changes to the protection of electronic PHI occur
- Before any new IT resource or data systems that may affect the handling or protection of PHI are implemented.

The ISO shall cause to perform this review following these steps, as adapted from the approach outlined in NIST SP 800-30 *Standards for Risk Analysis*:

<u>RISK ANALYSIS</u>

I. Identify Scope and Boundaries of the analysis
II. Gather data through interview, testing, observation, and review
III. Identify and document potential threats and vulnerabilities
IV. Assess the current security posture, measures, and mitigations
V. Determine the likelihood of a threat occurrence
VI. Determine the potential impact of a threat occurrence
VII. Determine the level of risk
VIII. Identify security measures, recommendations, or mandates, and finalize documentation in the POA&M

3.3 Annual FISMA Assessment

The *DHHS-2013-001 DHHS IT Security Policy* is based on the NIST 800-53 *Security Controls* framework. This framework also makes up the fundamental security requirements of the IRS regulation 1075. As such, DHHS is required to conduct an annual review of the DHHS infrastructure to ensure compliance with these standards. The format and approach for this review is based on the Federal Information Security Management Act (FISMA). The security controls that are to be inspected are organized into 17 control families within three classes (management, operational, and technical). These families are aligned with the security control areas specified in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems.*

The ISO shall cause to perform an annual FISMA assessment. Each assessment should cover at least 1/3 of the control areas, such that over a three-year timeframe all control areas will have been assessed. Although it is allowable for the ISO to conduct the review using internal resources, it is required to maintain a level of independence and objectivity during the review. Therefore, it is recommended that periodically this review be performed by a third party organization.

This review shall be conducted for each major system used within DHHS, and shall include all infrastructure and peripheral processes that are used by DHHS. Guidebooks and review templates can be found at:

http://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/ARS.pdf

FISMA Security Control Areas

Family	Class	Description
Access Control (AC)	Technical	The standards listed in this section focus on how the organization shall limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.
Awareness and Training (AT)	Operational	The standards listed in this section focus on how the organization shall: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned IS-related duties and responsibilities.
Audit and Accountability (AU)	Technical	The standards listed in this section focus on how the organization shall: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information

		system users can be uniquely traced to those users so they can be held accountable for their actions.
Security Assessment and Authorization (CA)	Management	The standards listed in this section focus on how the organization shall: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.
Configuration Management (CM)	Operational	The standards listed in this section focus on how the organization shall: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.
Contingency Planning (CP)	Operational	The standards listed in this section focus on how the organization shall establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.
Identification and Authentication (IA)	Technical	The standards listed in this section focus on how the organization shall identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.
Incident Response (IR)	Operational	The standards listed in this section focus on how the organization shall: (i) establish an operational incident handling capability

		for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.
Maintenance (MA)	Operational	The standards listed in this section focus on how the organization shall: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
Media Protection (MP)	Operational	The standards listed in this section focus on how the organization shall: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.
Physical and Environmental Protection (PE)	Operational	The standards listed in this section focus on how the organization shall: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.
Planning (PL)	Management	The standards listed in this section focus on how the organization shall develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.
Personnel Security (PS)	Operational	The standards listed in this section focus on how the organization shall: (i) ensure that individuals occupying positions of

		responsibility within organizations (including third party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.
Risk Assessment (RA)	Management	The standards listed in this section focus on how the organization shall periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.
System and Services Acquisition (SA)	Management	The standards listed in this section focus on how the organization shall: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate IS considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.
System and Communications Protection (SC)	Technical	The standards listed in this section focus on how the organization shall: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective IS within organizational information systems.
System and Information Integrity (SI)	Operational	The standards listed in this section focus on how the organization shall: (i) identify, report, and correct information and information system flaws in a timely manner;

		(ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories, and take appropriate actions in response.

Some Controls, Enhancements, Implementation Standards and Guidance, or portions thereof, only pertain to narrowly-defined types of data, such as Protected Health Information (PHI), Personally Identifiable Information (PII) or Federal Tax Information (FTI). Additionally, some requirements may only apply within specific implementation scenarios. The approved migration of data into a FedRAMP-approved Cloud Service Provider (CSP) for instance, may require the unique application of specific Controls, Enhancements, Implementation Standards or Guidance that are only applicable in this specific scenario. These specialized requirements are referenced and clearly documented in guidance material.

3.4 Random Risk Assessments

Random risk assessments will be performed at the discretion of the ISO, typically when circumstances require additional oversight, such as after a security incident, increased security threat, or significant changes to the IT infrastructure. These assessments are flexible in nature, and are intended to review specific elements that have been identified as exception-based or high priority. These reviews can also be performed to validate the appropriate remediation or mitigation of a previous finding.

The ISO shall document the business area, reason for the random review, scope of inspection, and dates of the review in the POA&M documentation. All findings and results will also be documented in the POA&M.

4.0 Revision History

Legal Review – 09-23-2013
Policy Approved – 09-30-2013

Signature:

Date: 9/30/2013

Eric Henrichsen
Information System & Technology Administrator
Nebraska Department of Health & Human Services