NEW YORK STATE | Department of Health | Office of Health Insurance Programs

OHIP DOH

System Security Plan (SSP)

Workbook Instructions

Version 1.2

September 18, 2015

Table of Contents

Introduction

New York State Office of Health Insurance Programs – Division of Systems (OHIP-DOS) is responsible for providing guidance and oversight for Medicaid-related information systems at the DOH. This responsibility includes defining business, information, and technical guidance that will create a common baseline and standards for these IT system implementation activities.

Purpose

This document provides guidance and instruction for individuals tasked with the responsibility of filling out the system security workbooks. The workbook identifies the required controls that must be documented and implemented as part of the organization's system security plan.

Requirement Sections Overview

1. Control Section

   This section defines the control requirement.

2. Guidance Section

   If present, provides an explanation of the policies, procedures, and practices required for the control to be considered implemented and effective.

3. Reference Section

   Provides information on applicable governance, from which the control requirement was derived.

4. Related Control Requirements

   If available, references control requirements in the SSP Workbooks that are related to the given control.

5. Assessment Procedure

   a. Assessment Objective

      Details the objectives that an assessor should consider when attempting to determine the existence and level of implementation of the control.

   b. Assessment Methods And Objects

Details the actions to be followed and the artifacts to be examined to ensure the control's existence and level of implementation

Completing the Control Implementation Sections

1. Understand the control requirements by reading the control and guidance sections. You may look up the items listed in the reference section for greater detail and background on the control.

2. Follow the assessment procedure to determine whether the control is or is not in place, and document the obtained results in the space provided.

3. When documenting a control that has been implemented, provide as much evidence and detail as possible. Examples may include artifacts such as:

   a. Policies, Guidelines, Standards, Procedures
   b. Process Maps
   c. Network Diagrams
   d. Organizational Charts
   e. System Architecture Documents
   f. System logs
   g. Screen shots
   h. Explanations of the practices in place

4. When documenting a control that does not exist, explain that the control, or parts of the control, is not currently in place.

   a. If the control or any part of the control is not in place, reference any compensating controls that may be in place to mitigate the risk.

   b. If there is a plan to put the control or any missing parts of the control in place, specify and include the expected implementation date.

5. Responsible for Control Implementation

   Document the organizational component or individual(s) responsible for supporting and maintaining the control.

6. Use the examples included in the next section for reference.

Workbook Examples

IA-2(2) - Network Access to Non-Privileged Accounts – Enhancement (Moderate) **P1**

Control

The information system implements multifactor authentication for network access to non-privileged accounts.

Reference(s): ***NYS ITS/EISO Policy & Standards***: NYS-P10-006 Identity Assurance Policy; NYS-S13-004 Identity Assurance Standard; NYS-S14-006 Authentication Tokens Standard; NYS-S14-013 Account Management/Access Control Standard	**Related Control Requirement(s):**

ASSESSMENT PROCEDURE: IA-2(2).1

Assessment Objective

Determine whether:
(i) The organization defines in the security plan, explicitly or by reference, the authentication level for the information system
(ii) The information system implements multifactor authentication for network access to non-privileged accounts

Assessment Methods And Objects

Examine: Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; list of non-privileged information system accounts; other relevant documents or records

Fully explain control implementation *(or fully explain why control requirement is not applicable)*

Status: IMPLEMENTED (all applicable systems)

Has the control been implemented completely, partially, planned, or not at all?

Applicability:

a. Primary Application and dependent Application “PHIReporter”
b. This control applies to all areas of the organization, including IT
c. This control does not apply to dependent Application “Widget” because of reason: *well-explained and credible business reason*

To which systems and parts of the organization do these controls apply [primary application, dependent application]? Name the applicable dependent applications if there are more than one. Include all relevant systems. Reference the information contained in the SSP overview tables, instead of re-stating the information here.

Description:

The organization has a defined and documented Information Security Plan: “POL-001 Organization Information Security Plan.” POL-001 references “STD-001 System Security Standard” for the level of authentication for network access to the system for non-privileged users.

High-level overview for documents and diagrams that satisfy the requirement. Be sure to identify whether the documents apply only to the primary system, to a dependent system, or to all.

Both Primary Application and dependent Application “PHI Reporters” adhere to POL-001 and STD-001.

Dependent application “PHIReporter” has an additional security Standard, “STD-016 PHI Reporting Standard.”

Detailed information to satisfy the requirement

STD-001 defines four levels of access for users, where three are non-privileged:

Role	Access type	Access to Sensitive Data	Access to PHI	Identity Assurance Level According to NYS-S13-004	Authentication Method
Executive	Read Only	No	No	IAL-2	Password
Level_1	Read, Modify, Create, No Delete	Yes	No	IAL-3	Two-factor authentication using RSA SecurID physical tokens
Level_2	Read, Modify, Create, Delete	Yes	Yes	IAL-3	Two-factor authentication using RSA SecurID physical tokens

RSA SecurID is an internally hosted multifactor authentication system that utilizes a physical token that generates a six-digit pseudo-random number once per minute, called a “key code.” The user is assigned a four-digit PIN at the time of account creation. To utilize the token with the Application, the user will enter his/her application user ID at the login prompt provided by the application. In the password box, instead of a memorized password, the user will prepend the key code with the PIN, resulting in a ten-digit “token code” that is then entered into the password box. The need for RSA SecurID is determined by a profile in the application, such that users who do not need SecurID for access can use the same login screen and enter a password. In the background, user passwords are validated against the Organization’s LDAP/Active Directory system, and SecurID token codes are validated against the RSA authentication database, using RADIUS. Maximum attempts, password strength, reset intervals, and other settings are defined in the STD-001.

Attachments: POL-001, STD-001, and STD-016 are attached to this SSP, for reference.

STD-001.docx POL-001.docx STD-016.docx

Attached or included documentation to support the statements made for control implementation. It is acceptable to either attach the documents directly to the workbook or include them as individual documents whose names are referenced in this section.

Responsible for Control Implementation: *(document the organizational component or contractor responsible for supporting and maintaining the control.)*

For Primary Application, the controls are supported internally by the Organization’s IT department. Dependent Application Organization’s ITS department is responsible for supporting and maintaining the applicable controls.

Reference the contact information in the Overview tables, instead of re-entering that information here. If additional contact information is required, detail the titles of the individuals responsible for control implementation, including roles. Include contact information.

SC-8(1) - Cryptographic or Alternate Physical Protection – Enhancement (High) P1

Control

The information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and detect changes to information during transmission, unless otherwise protected by defined alternative physical safeguards (defined in the applicable security plan).

Guidance

Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions that have common applications in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems.

Reference(s):	**Related Control Requirement(s):**
NYS ITS/EISO Policy & Standards: NYS-S14-003 Information Security Controls Standard, #18	SC-13

ASSESSMENT PROCEDURE: SC-8(1).1

Assessment Objective

Determine whether the information system implements cryptographic mechanisms to prevent unauthorized disclosure of information and to detect changes to information during transmission, unless otherwise protected by defined (in the applicable security plan) alternative physical safeguards.

Assessment Methods And Objects

Examine: System and communications protection policy; procedures addressing transmission integrity; information system design documentation; information system configuration settings and associated documentation; other relevant documents or records.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*

Status: IMPLEMENTED (all applicable systems)

Applicability:

a. Primary Application and Dependent Application “PHIReporter”
b. This control applies to PHI-Business-Area and PHI-Helpdesk.
c. This control does not apply to Secondary Application “Widget,” because of reason: *well-explained and credible business reason.*

Description:

The application resides in the Organization’s secure data center at One Organization Plaza, in City, State. The applicable network diagram is attached.

Since the application and its Network Attached Storage reside on a secure network in the Organization’s secure data center, there is no encryption employed between the servers for the application and the NAS infrastructure. Since they reside on separate network tiers, all communications between application layers are encrypted using TLS 1.1, with AES-256 encryption, and using valid digital certificates on each server and load balancer, as applicable. The SSL tunnels are terminated on the system’s dedicated F5 load balancers, for load balancing and redundancy. The traffic behind the load balancers is not encrypted, but the networks behind the F5s are logically segregated and isolated, and they are considered private to the application. The attached Visio network diagram depicts all termination points for the SSL between servers. All traffic must traverse the

F5s to reach the servers in question. The front-end of the application is web-based and exposed to the Internet. All connections to the application over the Internet use a web browser.

Firefox, IE, and Chrome are supported. User connection is via HTTPS with TLS 1.1. The web server uses a Verisign-issued valid digital certificate, as do all of the certificates for this app.

Attachments: System and communications protection policy POL-002 and Transmission Integrity Standard STD-002 are included for reference.

Network Diagram for Application.vsdx

POL-002.docx

STD-002.docx

Responsible for Control Implementation: *(document the organizational component or contractor responsible for supporting and maintaining the control.)*

The controls are supported internally by the organization. The Organization's ITS department is responsible for supporting and maintaining the applicable controls.

Additionally Responsibilities for Secondary Application "Widget."

James Brown, Architect (Supports and maintains application controls for the business)
(518) 555-1214, Mail Stop Five, One Organization Plaza, City, State, 00000

AC-2(7) - Role-Based Schemes – Enhancement (Moderate) P1

Control

(For CSP only) The organization:
(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;
(b) Monitors privileged role assignments; and
(c) Inspects administrator groups, root accounts and other system related accounts on demand, but at least once every fourteen (14) days to ensure that unauthorized accounts have not been created.

Guidance

(For CSP only) Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain security-relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, network and system administration, database administration, and web administration.

Reference(s):	**Related Controls Requirement(s):**

ASSESSMENT PROCEDURE: AC-2(7).1

Assessment Objective

Determine if:
(i) (For CSP only) the organization establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;

(ii) the organization monitors privileged role assignments;

(iii) (For CSP only) the organization inspects administrator groups, root accounts and other system related accounts on demand, but at least once during the specified period to ensure that unauthorized accounts have not been created.

Assessment Methods And Objects

Examine: (For CSP only) Procedures addressing account management; information system design documentation; information system configuration settings and associated documentation; information system-generated list of privileged user accounts and associated role; information system audit records; audit tracking and monitoring reports; other relevant documents or records.

Interview: (For CSP only) Organizational personnel with account management responsibilities.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*

Status: IMPLEMENTED (all applicable systems)

Applicability:

a. Primary Application and Secondary Application “PHIReporter”
b. This control applies to PHI-Business-Area.
c. This control does not apply to Secondary Application “Widget,” because of reason: *well-explained and credible business reason.*

Description:

Both primary application and dependent application “PHIReporter” utilize a role-based access scheme for assignment of privileges. There are four levels of privileged access within the application: Helpdesk, Security Coordinator, Approver, and SysAdmin. The entitlements assigned to these roles are respective of their assigned business responsibilities within the application and none have access to business-level ePHI. The mappings of roles to entitlements and business functions are included in the attached document “RolesResponsibilitiesPrimary.docx” and “RolesResponsibilitiesPHIReporter.docx”. The workflow diagram and approval procedure are attached, as is the de-provisioning procedure. A sample of the reports for comparing lists on-demand is also attached.

A system-managed automated workflow exists in both applications to request, approve, and assign access for both business users and all levels of privileged users. Logs are maintained for assignment activities through this workflow, and the actual users assigned to roles in the system are compared against the users assigned by the workflow, on a weekly basis. The workflow also handles our de-provisioning, so users that should not have access according to the workflow are disabled in the applications. IDs cannot be removed from the applications, as a design feature of the system that cannot be changed. It is possible to generate reports and compare these lists of users at any time, on-demand, as well.

Attachments:

RolesandResponsibilitiesPHIReporter.dc
RolesandResponsibilitiesPrimary.docx
Approval workflow.vsdx
PrivilegedUserAssuranceReport.xlsx
UserProvisioningProcedure.docx
UserDe-provisioningProcedure.docx

Responsible for Control Implementation: *(document the organizational component or contractor responsible for supporting and maintaining the control.)*

For Primary Application, the controls are supported internally by the Organization's IT department. Dependent Application Organization's ITS department is responsible for supporting and maintaining the applicable controls.

CM-2 – Baseline Configuration (Moderate) Assurance - P1

Control

The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.

Guidance

This control establishes baseline configurations for information systems and system components including communications and connectivity-related aspects of systems. Baseline configurations are documented, formally reviewed and agreed-upon sets of specifications for information systems or configuration items within those systems. Baseline configurations serve as a basis for future builds, releases, and/or changes to information systems. Baseline configurations include information about information system components (e.g., standard software packages installed on workstations, notebook computers, servers, network components, or mobile devices; current version numbers and patch information on operating systems and applications; and configuration settings/parameters), network topology, and the logical placement of those components within the system architecture. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems reflect the current enterprise architecture.

Reference(s): FISCAM: AS-3, CM-2; NIST SP: 800-128 ***NYS ITS/EISO Policy & Standards***: NYS-S14-008 Secure Configuration Standard, 4.0	**Related Controls Requirement(s):** CM-3, CM-6, CM-8, CM-9, PM-5, PM-7, SA-10

ASSESSMENT PROCEDURE: CM-2.1

Assessment Objective

Determine if:

(i) the organization develops and documents a baseline configuration of the information system;

(ii) the organization maintains, under configuration control, a current baseline configuration of the information system.

(iii) the organization documents deviations from the baseline configuration, in support of mission needs/objectives.

Assessment Methods And Objects

Examine: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the information system; enterprise architecture documentation; information system design documentation; information system architecture and configuration documentation; other relevant documents or records.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*

Status: IMPLEMENTED (all applicable systems)

Applicability:

a. Primary Application and Secondary Application “PHIReporter”
b. This control applies to all areas of the organization, including IT.
c. This control does not apply to Secondary Application “Widget,” because of reason: *well-explained and credible business reason.*

Description:

Configuration management standards for both applications are attached. A sample of the configuration profiles for Primary System and PHI Reporter are attached. A sample for the current list of exceptions for these applications, with respect to the standard, is attached.

Configuration changes are approved through a weekly meeting consisting of the IT manager and system admins and any deviations from the standards are documented.

Attachments:

STD-058.docx STD-057.docx ConfigurationExceptionLogPri.docx ConfigurationExceptionLogPHIR.docx

Responsible for Control Implementation: *(document the organizational component or contractor responsible for supporting and maintaining the control.)*

For Primary Application, the controls are supported internally by the Organization’s IT department. Dependent Application Organization’s ITS department is responsible for supporting and maintaining the applicable controls.

AU-2 – Audit Events (Moderate) P1

Control

The organization:

a. Determines, based on a risk assessment and CMS mission/business needs, that the information system is capable of auditing the events specified in Implementation Standard 1;

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines which events specified in Implementation Standard 2 require auditing on a continuous basis in response to specific situations.

Implementation Standard(s)

1. List of auditable events:

(a) Server alerts and error messages;

(b) User log-on and log-off (successful or unsuccessful); (c) All system administration activities;

(d) Modification of privileges and access; (e) Start up and shut down;

(f) Application modifications;

(g) Application alerts and error messages; (h) Configuration changes;

(i) Account creation, modification, or deletion; (j) File creation and deletion;

(k) Read access to sensitive information;

(l) Modification to sensitive information; and

(m) Printing sensitive information.

2. Subset of Implementation Standard 1 auditable events: (a) User log-on and log-off (successful or unsuccessful); (b) All system administration activities;

(c) Modification of privileges and access; and

(d) Account creation, modification, or deletion.

3. Verify that proper logging is enabled in order to audit administrator activities.

4. (For FTI only) Generate audit records for the following events in addition to those specified in other controls: (a) All successful and unsuccessful authorization attempts.

(b) All changes to logical access control authorities (e.g., rights, permissions).

(c) All system changes with the potential to compromise the integrity of audit policy configurations, security policy configurations and audit record generation services. (d) The audit trail shall capture the enabling or disabling of audit report generation services.

(e) The audit trail shall capture command line changes, batch file changes and queries made to the system (e.g., operating system, application, and database).

The organization defines the subset of auditable events from AU-2a to be audited. The events to be audited are approved and accepted by Joint Authorization Board (JAB).

5. (For CSP only) For service providers, this Standard replaces the above Control and Standards. The organization:

a. Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: successful and unsuccessful account logon events, account management events, object access, policy change, privilege functions, process tracking, and system events; and for Web applications: all administrator activity, authentication checks, authorization checks, data deletions, data access, data changes, and permission changes; and

b. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events;

c. Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and

d. Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: organization-defined subset of the auditable events to be audited continually.

Guidance

An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures.

Reference(s): FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(5)(ii)(C), 164.312(b); IRS-1075: 9.3#2.1; NIST SP: 800-92; Web: csrc.nist.gov/pcig/cig.html ***NYS ITS/EISO Policy & Standards***: NYS-S14-005 Security Logging Standard, 4.4c, Appendix A: Security Events to Log	**Related Controls Requirement(s):** AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, SI-4

ASSESSMENT PROCEDURE: AU-2.1

Assessment Objective

Determine if:

(i) the organization determines, based on a risk assessment and CMS mission/business needs, that the information system is capable of auditing the list of auditable events specified in the Implementation Standards;

(ii) the organization coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and help guide the selection of auditable events;

(iii) the organization defines in the security plan, explicitly or by reference, information system auditable events;

(iv) the organization determines the auditable events defined in Implementation Std.2 to be audited within the information system, and the frequency of (or situation requiring) auditing for each identified event.

(v) the organization provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents

(vi) the organization meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods And Objects

Examine: Audit and accountability policy; procedures addressing auditable events; security plan; information system configuration settings and associated documentation; information system audit records; list of information system auditable events; other relevant documents or records.

Interview: Organizational personnel with auditing and accountability responsibilities.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*

Status: IMPLEMENTED (all applicable systems)

Applicability:

a. Primary Application and Secondary Application “PHIReporter”
b. This control applies to all areas of the organization, including IT.
c. This control does not apply to Secondary Application “Widget,” because of reason: *well-explained and credible business reason.*

Description:

Risk Assessment procedure is based on NIST 800-30 and is attached. Latest report from the annual risk assessment of Primary App and PHI Reporter are attached. All activities are logged for privileged roles within both applications. Complete audible events standards are attached.

Events	Primary App	PHI Reporter
(a) Server alerts and error messages	Yes	Yes
(b) User log-on and log-off (successful or unsuccessful); (c) All system administration activities;	Yes	Yes
(d) Modification of privileges and access; (e) Start up and shut down;	Yes	Yes
(f) Application modifications;	**No**	**No**
(g) Application alerts and error messages; (h) Configuration changes;	Yes	Yes
(i) Account creation, modification, or deletion; (j) File creation and deletion;	Yes	Yes
(k) Read access to sensitive information;	Yes	Yes
(l) Modification to sensitive information; and	Yes	Yes
(m) Printing sensitive information.	Yes	Yes
2. Subset of Implementation Standard 1 auditable events: (a) User log-on and log-off (successful or unsuccessful); (b) All system administration activities;	Yes	Yes
(c) Modification of privileges and access; and	Yes	Yes
(d) Account creation, modification, or deletion.	Yes	Yes

Attachments:

Risk assessment procedure.docx

RA Report PrimaryApp 2015.do

RA Report PHIReporter 2015.dc

STD-0044.docx

Responsible for Control Implementation: *(document the organizational component or contractor responsible for supporting and maintaining the control.)*

For Primary Application, the controls are supported internally by the Organization's IT department. Dependent Application Organization's ITS department is responsible for supporting and maintaining the applicable controls.

RA-3 – Risk Assessment (Moderate) Assurance - P1

Control

The organization:
a. Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;
b. Documents risk assessment results in the applicable security plan;
c. Reviews risk assessment results within every three hundred sixty-five (365) days;
d. Disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO; and
e. Updates the risk assessment before issuing a new ATO package or within every three (3) years, whichever comes first; or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.

Implementation Standard(s)

1. (For CSP only) For service providers, the organization documents risk assessment results in the security assessment report.

2. (For CSP only) For service providers, the organization reviews risk assessment results at least every three (3) years or when a significant change occurs.

Guidance

Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems.
Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring.
RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which includes security control supplementation.
(For CSP only) Significant change is defined in NIST Special Publication 800-37 Revision 1, Appendix F.

Reference(s): FISCAM: AS-1, SM-2; HIPAA: 164.308(a)(1)(ii)(A), 164.308(a)(1)(ii)(B), 164.316(a); HSPD 7: D(8), F(19); IRS-1075: 6.3.3#2, 9.14#1.3; NIST SP: 800-30, 800-39; OMB: M-04-04; Web: idmanagement.gov ***NYS ITS/EISO Policy & Standards***: NYS-P02-003 Information Security Policy, 4.4, 4.9.a, 4.11.c.8; NYS-S14-001 Information Security Risk Management Standard, 4.0	**Related Controls Requirement(s):** PM-9, RA-2

ASSESSMENT PROCEDURE: RA-3.1

Assessment Objective

Determine if:
(i) the organization conducts an assessment of risk of the information system and the information it processes, stores, or transmits that includes the likelihood and magnitude of harm, from the unauthorized:
- access;
- use;
- disclosure;
- disruption;
- modification; or
- destruction;

(ii) the organization reviews and updates the risk assessment policy and procedures within every three hundred sixty-five (365) days. (iii) the organization reviews risk assessment results within every three hundred sixty-five (365) days;

(v) the organization updates the risk assessment before issuing a new ATO package or within every three (3) years, whichever comes first, or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security or authorization state of the system.

(vi) (For CSP only) the organization meets all the requirements specified in the applicable Implementation Standard(s).

(iv) the organization disseminates risk assessment results to affected stakeholders, Business Owners(s), and the CMS CISO;

Assessment Methods And Objects

Examine: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records.

Interview: Organizational personnel with risk assessment responsibilities.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*

Status: IMPLEMENTED (all applicable systems)

Applicability:

a. Primary Application and Secondary Application “PHIReporter”
b. This control applies to all areas of the organization, including IT.
c. This control does not apply to Secondary Application “Widget,” because of reason: *well-explained and credible business reason.*

Description:

The Organization has a documented risk assessment process that conforms to NIST 800-30. Assessments include the assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. Reports of the assessment are presented to Organization leadership when complete and remediation plans are developed and tracked to completion for identified issues. The Risk assessment process has a procedure for accepting risk that requires signoff of the business owner, ISO, and the CIO.

Currently, risk assessment results are reflected in the Organization’s existing security plan for the applications, but moving forward, this will be done for the SSP workbooks, as well. Risk assessments are conducted annually. Risk assessments are required to be formally performed, prior to any PHI system being implemented. Assessments are revisited more frequently, should a threat surface that applies to our systems or in the unfortunate occurrence of a breach.

Attachments:

RA Report PrimaryApp 2015.do

RA Report PHIReporter 2015.dc

Risk assessment procedure.docx

If these documents are already attached to the workbook, it is preferable to reference the control that has the attachments included, rather than attaching repetitively.

Responsible for Control Implementation: *(document the organizational component or contractor responsible for supporting and maintaining the control.)*

For Primary Application, the controls are supported internally by the Organization’s IT department. Dependent Application Organization’s ITS department is responsible for supporting and maintaining the applicable controls.

IR-2 – Incident Response Training (Moderate) Assurance - P2

Control

The organization provides incident response training to information system users consistent with assigned roles and responsibilities:
a. Within ninety (90) days of assuming an incident response role or responsibility;
b. When required by information system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

Guidance

Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources.

Reference(s): FISCAM: AC-5, AS-2; HIPAA: 164.308(a)(6)(i); IRS-1075: 9.9#2.1-2; NIST SP: 800-16, 800-50 ***NYS ITS/EISO Policy & Standards***: NYS-P03-002 Information Security Policy, 4.2.e.6; NYS-S13-005 Cyber Incident Response Standard, 4.0 Step 1, Appendix A	**Related Controls Requirement(s):** AT-3, CP-3, IR-8

ASSESSMENT PROCEDURE: IR-2.1

Assessment Objective

Determine if:
(i) the organization identifies personnel with incident response roles and responsibilities with respect to the information system;

(ii) the organization provides incident response training to information system users consistent with assigned roles and responsibilities;

(iii) incident response training material addresses the procedures and activities necessary to fulfill identified organizational incident response roles and responsibilities;

(iv) the organization defines in the security plan, explicitly or by reference, the frequency of refresher incident response training in accordance with organization-defined frequency;

(v) the organization provides refresher incident response training in accordance with organization-defined frequency.

Assessment Methods And Objects

Examine: Incident response policy; procedures addressing incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records.

Interview: Organizational personnel with incident response training and operational responsibilities.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*

Status: IMPLEMENTED (all applicable systems)

Applicability:

a. Primary Application and Secondary Application “PHIReporter”
b. This control applies to all areas of the organization, including IT.
c. This control does not apply to Secondary Application “Widget,” because of reason: *well-explained and credible business reason.*

Description:

Users are provided incident response training consistent with assigned roles and responsibilities, according to the attached Incident Response plan.

New hires and new users of the applications are provided training on the incident response procedure, prior to gaining access to the applications.

Changes to the incident response plan are communicated to users quarterly and online training is made available and tracked (sample record of completed training is provided).

All users are required to complete incident response training on an annual basis.

Incident response training for privileged users and business users are attached.

Attachments:

Sample of record for completed traini

Incident Response Plan.docx

Incident Response Training.pptx

Privileged Incident Response Training.p

Responsible for Control Implementation: *(document the organizational component or contractor responsible for supporting and maintaining the control.)*

For Primary Application, the controls are supported internally by the Organization’s IT department. Dependent Application Organization’s ITS department is responsible for supporting and maintaining the applicable controls.

AT-2 – Security Awareness Training (Moderate) Assurance - P1

Control

The organization provides basic security awareness training to information system users (including managers, senior executives, and contractors):
a. As part of initial training for new users prior to accessing any system's information;
b. When required by system changes; and
c. Within every three hundred sixty-five (365) days thereafter.

Implementation Standard(s)

1. An information security and privacy education and awareness training program is developed and implemented for all employees and individuals working on behalf of CMS involved in managing, using, and/or operating information systems.
2. Privacy awareness training is provided before granting access to systems and networks, and within every three hundred sixty-five (365) days thereafter, to all employees and contractors, to explain the importance and responsibility in safeguarding PII and ensuring privacy, as established in Federal legislation and OMB guidance.

Guidance

Organizations determine the appropriate content of security and privacy awareness training, and security and privacy awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content includes a basic understanding of the need for information security and user actions to maintain security and privacy, and to respond to suspected security and privacy incidents. The content also addresses awareness of the need for operations security and privacy as it relates to CMS' information security program. Security and privacy awareness techniques can include, for example, displaying posters, offering supplies inscribed with security and privacy reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security and privacy awareness events.

Reference(s): Executive Order: 13587; FISCAM: AS-1, SM-4; HIPAA: 164.308(a)(5)(i), 164.308(a)(5)(ii)(A), 164.308(a)(5)(ii)(B); IRS-1075: 6.2#1.1-2, 9.4#1.2; NIST SP: 800-50 ***NYS ITS/EISO Policy & Standards***: NYS-P03-002 Information Security Policy, 4.7.a	**Related Controls Requirement(s):** AT-3, AT-4, PL-4

ASSESSMENT PROCEDURE: AT-2.1

Assessment Objective

Determine if:
(i) the organization provides basic security awareness training to information system users (including managers, senior executives, and contractors) as part of initial training for new users and when required by system changes;
(ii) the organization defines in the security plan, explicitly or by reference, the frequency of refresher security awareness training and the frequency is at least every three hundred sixty-five (365) days;

(iii) the organization provides refresher security awareness training in accordance with the organization-defined frequency.
(iv) the organization meets all the requirements specified in the applicable Implementation Standard(s).

Assessment Methods And Objects

Examine: Security and privacy awareness and training policy; procedures addressing security and privacy awareness training implementation; appropriate codes of federal regulations; security and privacy awareness training curriculum; security and privacy awareness training materials; security plan; training records; other relevant documents or records.

Interview: Organizational personnel comprising the general information system user community.

Fully explain control implementation *(or fully explain why control requirement is not applicable)*

Status: NOT IMPLEMENTED (all applicable systems)

Applicability:

a. Primary Application and Secondary Application “PHIReporter”
b. This control applies to all areas of the organization, including IT.
c. This control does not apply to Secondary Application “Widget,” because of reason: *well-explained and credible business reason.*

Description:

The organization does NOT currently provide security awareness training to users of Primary Application or dependent application PHIReporter.

It is anticipated that security awareness efforts will concentrate on security incidents in our industry, including any security issues identified within our own organization. This will be complimented by the OWASP Top 10 threats, Online PHI awareness training from industry leader “LeaderPHITrainer” and an organization-wide phishing and spear-phishing testing, conducted by that same vendor. Information on the vendor is attached. Monthly security awareness emails will be distributed to all workers, including contractors, employees and leadership. Training will be conducted at time of hire and annually, thereafter. Training will also be reinforced following phishing exercises and in the occurrence of a breach or other adverse security event. Vendors are required in their BAAs to perform the same.

A project plan with dates and assignments for tasks has been attached, for the development of a comprehensive security awareness program. The program is expected to begin piloting awareness efforts in November, 2015, with an anticipated go-live in February, 2015.

Attachments:

Security Awareness Project Plan.mpp

Information on LeaderPHITrainer.do

Responsible for Control Implementation: *(document the organizational component or contractor responsible for supporting and maintaining the control.)*

For Primary Application, the controls are supported internally by the Organization’s IT department. Dependent Application Organization’s ITS department is responsible for supporting and maintaining the applicable controls.