HITRUST CSF® Assurance Program Documentation Requirements

Last updated: 5/14/19

Purpose

This document defines the expectations for the documentation of HITRUST CSF Assurance Program Validated Assessments. These requirements are designed to ensure the consistency and quality of documenting work during a Validated Assessment by a HITRUST CSF Assessor Organization and to increase the quality of and streamline the HITRUST Quality Assurance (QA) process.

Pre-Assessment Planning

The purpose of pre-assessment planning is to ensure that the HITRUST CSF Assessor understands the scope of the assessment and designs appropriate testing procedures that address the understood scope. Some of the areas that need to be understood and documented during the planning phase are:

- Systems, business processes, and physical locations to be assessed
- Risk Factors to be assessed against
- Populations to be tested
    - Users
    - Endpoints
    - Network Devices
    - Mobile Devices
- Identification of control requirements that may have a shared responsibility

Once these items are understood a test plan should be developed that addresses all aforementioned areas.

Test Plan

The test plan is the blueprint for the performance of a HITRUST CSF Assessment. It should include test procedures for each maturity domain for each control requirement in the HITRUST CSF Assessment. It should also include details on any sampling that is used for testing to include total population and sample size as well as how the sample is to be selected (random, systematic); if this sampling information is not captured in the test plan, it should be captured in the working paper used to document the sample test. Test plans should also include who the Engagement Executive and Engagement Lead, and Engagement QA Reviewer are for the HITRUST CSF Assessment. The test plan should be signed-off by the Engagement Executive and Engagement lead and optionally by the QA Reviewer.

General guidance for test procedures by maturity domain are:

- Policy – Documentation review
- Procedure – Interview, process flow diagram, runbook
- Implementation – Observation of control applied to a population or sample thereof

- Measured – Review of documentation for operational, independent measures and metrics
- Managed – Observation of mechanism used to track adjustments identified by measurements

Working paper documentation

Working papers are used to document testing that is performed during a HITRUST CSF Assessment. The working papers should include copies of policies and procedures, process flow diagrams, or spreadsheets used to document a sample and test results. Working papers are expected to have the following required information on them:

- Name of Assessment
- Name of person that performed the test/review
- Date the test was performed
- Description of test procedure
- Result of test procedure

Working papers submitted during the HITRUST QA process that do not contain the required information will result in the HITRUST CSF Assessment being reverted back to the HITRUST CSF Assessor for proper documentation.

Example Test Plan

Validated Assessment Test Plan
Entity: Chinstrap Penguin
Last updated: 11/10/XX

Engagement Executive	John Smith
Engagement QA	Jane McDonald
Engagement Lead	Sandra Jones

			Planned Tests				
Domain	**Requirement Statement**	**ID**	Policy	Process	Implemented	Measured	Managed
4 - MDM	Remote access is limited only to information resources required by users to complete job duties.	0417.01y3Organizational.5	Inspect written policies related to teleworking to determine whether the remote access is limited only to information resources required by home users to complete job duties. If no written policy or standard exists, determine is an ad hoc or informal policy around this requirement statement is observed in practice.	Inspect written procedures to determine whether written procedures address this requirement statement and the elements outlined in the associated policy. If no written procedure exists, determine is an ad hoc or informal procedure around this requirement statement is observed in practice.	Obtain from the remote access solution used by the organization the listing of individuals with the ability to remotely connect to network resources. Select a sample of accounts / users with remote access privileges, and for each inspect user access request documentation to evidence that their remote access privileges were formally requested and approved by management at time of issuance.	Select a sample of periodic reviews of remote access privileges to determine whether such access is formally reviewed and approved by management at a fixed cadence.	(N/A, Assessor.io understands through planning discussions with Chinstrap Penguin personnel that processes were not in place to formally and consistently manage, investigate, and consistently resolve issues related to this requirement statement's performance.)
4 - MDM	The organization prohibits the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting).	0429.01x1System.14	Inspect written policies and/or standards related to mobile computing & communications and determine if the organization prohibits the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting). If no written policy or standard exists, determine is an ad hoc or informal policy around this requirement statement is observed in practice.	Inspect written procedures to determine whether written procedures address this requirement statement and the elements outlined in the associated policy. If no written procedure exists, determine is an ad hoc or informal procedure around this requirement statement is observed in practice.	- Obtain from the IT asset inventory, CMDB, or similar sources the population of company-issued mobile devices. Select a sample, and for each inspect evidence that the organization's centralized MDM solution was implemented and is operational. - Inspect the mobile device management configuration settings and confirm that the solution prohibits the circumvention of built-in security controls through means such as jailbreaking or rooting.	(N/A, Assessor.io understands through planning discussions with Chinstrap Penguin personnel that measures and metrics are not in place to monitor the performance of this control requirement.)	(N/A, Assessor.io understands through planning discussions with Chinstrap Penguin personnel that measures and metrics are not in place to monitor the performance of this control requirement.)
4 - MDM	The organization ensures that mobile devices connecting to corporate networks, or storing and accessing company information, allow for remote wipe.	0428.01x2System.3	Inspect written policies to ensure appropriate coverage of this requirement statement. If no written policy or standard exists, determine is an ad hoc or informal policy around this requirement statement is observed in practice.	Inspect written procedures to determine whether written procedures address this requirement statement and the elements outlined in the associated policy. If no written procedure exists, determine is an ad hoc or informal procedure around this requirement statement is observed in practice.	Inspect the mobile device management configuration settings and confirm that the MDM solution provides remote wipe capabilities.	(N/A, Assessor.io understands through planning discussions with Chinstrap Penguin personnel that measures and metrics are not in place to monitor the performance of this control requirement.)	(N/A, Assessor.io understands through planning discussions with Chinstrap Penguin personnel that measures and metrics are not in place to monitor the performance of this control requirement.)

Example Sampling Working Paper

Validated Assessment Sampling Leadsheet #6_15a
Client: Chinstrap Penguin

Performed by:	Larry Samuel
Performed on:	Oct. 24, 20XX

Test Procedure:	Inspected AV details for a sample of 6 endpoints for presence of anti-virus software, DAT file version, and last scan date and compared this information to the AV management console.
Test Result:	One of a sample of 6 workstations was not scanned for viruses in over five months. Exception noted.
Sampling Info:	- Population source: IT asset inventory maintained in SharePoint - Population date range: N/A to this test - Population size: 58 endpoints - Population completeness: Completeness of the IT asset inventory used for sampling was verified as part of testing a separate control requirement; see 0701.07a1Organizational.12. - Sampling method: Random - Minimum required sample size per HITRUST's sampling guidance: 6 (at least 10% of the population)

	AV Details Reported on the Endpoint			AV Details Reported on the AV Management Console				
Sampled Endpoint	Was Anti-Virus Installed and enabled?	Anti-Virus Pattern Version	Last Scan Date	Last Report Date	Anti-Virus Version	Last Scan Date	**Conclusion**	**Screenshot Evidence Link**
PC1	Yes	14.926.0	10/18/20XX	10/18/20XX	14.926.0	10/18/20XX	No issues noted	Screenshots for all samples in workpaper "Domain 6 - AV_Samples.docx"
PC2	Yes	14.926.0	10/18/20XX	10/18/20XX	14.926.0	10/18/20XX	No issues noted	
PC3	Yes	14.926.0	10/18/20XX	10/18/20XX	14.926.0	10/18/20XX	No issues noted	
PC4	Yes	14.926.0	10/18/20XX	10/18/20XX	14.926.0	10/18/20XX	No issues noted	
PC5	Yes	14.926.0	10/18/20XX	10/18/20XX	14.926.0	10/18/20XX	No issues noted	
PC6	Yes	14.765.2	5/13/20XX	5/14/20XX	14.765.2	5/12/20XX	PC has not scanned in over 5 months	

Example Artifact Working Paper

Validated Assessment Workpaper 5.1_05

Domain: 5- Wireless Security

Assessment: Chinstrap Penguin

Requirement Statement: 0502.09m1Organizational.5

PBC: Assessor.io observed this evidence being pulled during on-site walkthroughs with Jonathan Seagull on 11-19-XX

Tested: LM on 11-19-XX

Test procedure: Inspect wireless access point configuration settings to ensure that wireless networks are configured with strong encryption (AES WPA2 at a minimum).

Test Result: No findings. Chinstrap Penguin's wireless network was configured to use strong encryption.