HITRUST

Evaluating Control Maturity Using the HITRUST Approach

Quasi-quantitative scoring based on the HITRUST CSF security and privacy control implementation maturity model

v.HT-1602-02

September 2020

Executive Summary

HITRUST®, since 2007, has been championing and delivering solutions to address the lack of a common understanding around the security and privacy controls needed to safeguard sensitive information and individual privacy. These solutions include:

(1) An industry accepted information security and privacy control framework, the HITRUST CSF®, that incorporates multiple regulatory requirements and best practice standards and frameworks;
(2) A standard, open, and transparent assessment process to provide accurate, consistent, and repeatable assurances around the level of protection provided by an organization; and
(3) An industry recognized certification of an organization's conformity to the protection requirements specified in the HITRUST CSF through the HITRUST CSF Assurance Program™.

This guide provides updated guidance for the assessment of HITRUST CSF control requirements using the HITRUST CSF control maturity model, evaluation, and scoring approach as well as the use of organizational- and requirement statement-level criteria and requirement statement-specific illustrative procedures to build out the test plans needed to conduct a successful CSF assessment.

HITRUST also provides a more robust version of its original HITRUST CSF control maturity scoring rubric by addressing each level of the HITRUST CSF maturity model independently. This greatly expanded rubric will help ensure internal and external assessors apply HITRUST assessment guidance appropriately and improve internal and external consistency of maturity ratings and scores.

A copy of the most current version of the HITRUST CSF control maturity scoring rubric can be downloaded from the HITRUST Website's download page for CSF Assurance & Related Programs.

Contents

Table of Contents

List of Figures

List of Tables

Introduction

HITRUST champions and delivers solutions to address the lack of a common understanding around the security and privacy controls needed to demonstrate an appropriate level of due diligence and due care for the protection of sensitive information, as well as a common mechanism for providing assurances for both internal and external stakeholders around the state of an organization's information risk management and compliance program. Central to this common mechanism for providing assurances is the guidance HITRUST provides on evaluating the maturity of a HITRUST CSF control's implementation.

In many cases assessors evaluate controls solely based on whether they are in place or implemented, resulting in a very binary, compliance-oriented approach. Models in which partial implementation is noted are arguably more useful, but they also fail to provide an adequate view of organizational risk.

Financial and information technology auditors address this issue by evaluating control effectiveness and its two components: design effectiveness and operational effectiveness. The first, design effectiveness, refers to how well a control is designed to address a specific control objective, i.e., the risk it was designed to control. The second, operational effectiveness, addresses whether controls consistently operate over time as designed, i.e., if they continue to effectively address the risks they were designed to control.

HITRUST takes this concept of effectiveness and applies it through the lens of process maturity; however, rather than evaluate the maturity of a specific process, assessors evaluate the effectiveness of a control's implementation through the achievement of specific maturity levels in the model that describe important aspects of an organization's control implementation.

HITRUST CSF Control Maturity Model

HITRUST's approach to evaluating a control's implementation is based on a control maturity model outlined by the National Institute of Standards and Technology (NIST) Program Review of Information Security Management Assistance (PRISMA),[i] which provides five levels of maturity roughly similar to the Carnegie Melon Software Engineering Institute's (CM-SEI's) Capability Maturity Model Integrated (CMMI) process improvement model.[ii]

"The structure of a PRISMA Review is based upon the [CMMI], where an organization's developmental advancement is measured by one of five maturity levels"[iii]: (1) *Policies* (does the organization know what it needs to do?), (2) *Procedures* (does the organization know how to do it?), (3) *Implementation* (has the organization done it?), (4) *Testing* (does the organization ensure it is working properly?), and (5) *Integration* (are the activities in the first four levels well integrated?).[iv] Assessing the maturity of an organization's information protection program by leveraging a comprehensive and consistently applied methodology, including assessing the status of its information security policies, procedures, and controls implementation, provides better assurance because it's based on direct rather than circumstantial evidence and therefore is more indicative of the actual level of protection the organization provides sensitive information, making it the only legitimate method of measuring an organization's information risk profile.

Like the PRISMA model, the HITRUST model's first three levels provide rough equivalence with traditional compliance-based assessments. First, control requirements must be clearly understood at all levels of the organization through documented policies or standards that are communicated with all stakeholders. Second, procedures must be in place to support the actual implementation of required controls. These first two levels essentially address the concept of design effectiveness. Third, the controls must be fully implemented and tested as required to ensure they operate as intended. HITRUST then modified the PRISMA model to specifically address the concept of 'you can't manage what you don't measure' in the fourth and fifth levels of the model, and it's these last three levels that support the evaluation of a control's operational effectiveness.

The initial maturity level, *Policy*, considers the existence of current, documented information security policies or standards in the organization's information security program and whether they fully address the control's implementation specifications. For example, if a requirement statement has multiple actions associated with it, does a corporate policy or standard address all its elements, either directly in the policy or indirectly by reference to an external standard? And does the policy apply to all organizational units and systems within scope of the assessment?

The second maturity level, *Procedures*, considers the existence of documented procedures or processes developed from the policies or standards and whether they reasonably apply to the organizational units and systems within scope of the assessment. For example, are there one or more written procedures that address the implementation of all the elements specified in a requirement statement?

The third maturity level, *Implemented*, considers the actual implementation of the policies and whether the control's implementation specifications are applied to all the organizational units and systems within scope of the assessment. For example, are all elements of a requirement statement addressed by the implementation for all corporate shared services?

The fourth maturity level, *Measured*, considers the testing or measurement (metrics) of the specification's implementation and whether they continue to remain effective. This idea of monitoring is not new, as the American Institute of Certified Public Accountants[v] (AICPA) lists monitoring, i.e., the process of assessing

performance over time, as one of five interrelated components of internal control. However, the concept of continuous monitoring, upon which this level is based, is relatively new.

NIST equates continuous monitoring with maintaining ongoing awareness to support organizational risk decisions. The terms 'continuous' and 'ongoing' in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. Thus, testing of the control to support an annual assessment or audit will likely not satisfy this requirement for many if not most controls. Instead, an organization must periodically (and possibly aperiodically) measure and track this information over time. For example, an organization may use a management console to track antivirus software implementation status in near real-time and produce metrics of the percentage of end-user devices that have the latest software and signature updates.

The highest maturity level, *Managed*, reviews the organization's management of its control implementations based on these metrics. For example, if common or special variations are discovered through testing or measurement of a control's effectiveness, can the organization demonstrate it has a management process for this metric and, when general or special variations occur, can it show it has performed a root cause analysis and taken corrective action based on the results?

Evidence suggests that the more mature an organization's information protection program—specifically their information security controls which demonstrate proficiency of operation, management, and reporting—the more likely an organization will be to continue to operate those controls in a similar manner in the future. Further, it can also be shown that mature organizations are less likely to suffer a breach and, should a breach occur, the more likely these organizations will be able to contain it and minimize the impact. This is because controls that have been implemented at a high level of maturity are simply less likely to fail than controls that are implemented poorly. For example, Forrester Consulting has shown organizations that implement a CMM-based maturity model and have the highest level of maturity—even when limited to the area of identity and access management—incur roughly "half the number of breaches as the least mature … [and save] 40% in technology costs and an average of $5 million in breach costs."[vi]

Evaluating HITRUST CSF Controls

Providing Organizational Context for Use of the Maturity Model

To help provide additional context for an assessor's evaluation of a control's maturity, the following table provides a bulleted list of evaluation criteria needed for an organization to fully achieve each of the five HITRUST maturity levels:[vii]

Table 1. Organizational-level Evaluation Criteria

Maturity Level	Organizational-level Evaluation Criteria
Policy	• Formal, up-to-date documented policies or standards stated as "shall" or "will" statements exist and are readily available to employees • Policies establish a continuing cycle of assessing risk and implementation as well as uses monitoring for program effectiveness • Policies are written to cover all facilities and operations and/or systems within scope • Policies are approved by key affected parties • Policies delineate the information security management structure, clearly assign security responsibilities, and lay the foundation necessary to reliably measure progress/compliance • Policies or standards identify specific penalties/disciplinary actions if the policy not followed
Procedure	• Formal, up-to-date, documented procedures are provided to implement the security controls identified by the defined policies • Procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed • Procedures clearly define information security responsibilities and expected behaviors for (1) asset owners and users, (2) information resources management and information technology personnel, (3) management, and (4) information security administrators • Procedures identify the individuals to be contacted for further information or guidance • Procedures document the implementation of and the rigor in which the control is applied • Procedures are communicated to individuals who are required to follow them
Implemented	• Information security procedures and controls are implemented in a consistent manner everywhere that the procedure applies and are reinforced through training • Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged • Initial testing is performed to ensure controls are operating as intended
Measured	• Tests are routinely conducted to evaluate the adequacy and effectiveness of all implementations • Tests ensure that all policies, procedures, and controls are acting as intended and that they provide an appropriate level of information security • Self-assessments[viii] are routinely conducted to evaluate the adequacy and effectiveness of all implementations • Independent audits are an important check on organization performance, but are not to be viewed as a substitute for evaluations initiated by organizational management • Information gleaned from records of potential and actual Information security incidents and security alerts, e.g., those issued by software vendors, are considered measurements, help identify specific vulnerabilities, and provide insights into the latest threats and resulting risk • Threats are continually re-evaluated • Evaluation requirements, including requirements regarding the type and frequency of testing, are documented, approved, and effectively implemented • The frequency and rigor with which individual controls are tested depend on the risks that will be posed if the controls are not operating effectively • Costs and benefits of information security are measured as precisely as practicable • Status metrics for the information security program as well as individual information security investment performance measures are established

Maturity Level	Organizational-level Evaluation Criteria
Managed	• Effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual information security incidents or through information security alerts issued by US-CERT, vendors, and other trusted sources • Policies, procedures, implementations, and tests are continually reviewed, and improvements are made • Information security is integrated into capital project/budget planning processes • An active enterprise-wide information security program achieves cost-effective information security • Security vulnerabilities are understood and managed • Controls are adapted to emerging threats and the changing information security environment • Decision-making is based on cost, risk, and mission impact • Additional or more cost-effective security alternatives are identified as the need arises • Status metrics for the information security program as well as individual information security investment performance measures are met

By understanding these general requirements, assessors are better prepared to assess the maturity of a HITRUST CSF control's implementation.

Adapting CSF Controls for Assessment Against the Model

Since the HITRUST CSF is structured on the International Standards Organization (ISO) information security standard,[ix] the CSF's control implementation specifications consist of various policy, process, and other requirement statements. Therefore, the language had to be modified slightly within MyCSF™[x] to ensure the requirement statements used for a HITRUST CSF Assessment[xi] lent themselves to PRISMA's approach for the evaluation of control effectiveness.

For this reason, HITRUST CSF Assessments are based on the evaluation of requirement statements derived from the implementation specifications in the HITRUST CSF rather than on the actual language contained in the CSF. The intent is to focus on actionable requirements rather than on any policy or process requirements contained in the specifications. However, while the requirement statements used in MyCSF are derivations of the CSF content, *assessors must address all the actionable requirements contained in the CSF when evaluating each requirement statement*.

For example, CSF control 01.a, Access Control Policy, states "the organization shall develop, disseminate, and review and update the access control policy and procedures annually." Rather than associate this requirement statement with 01.a, it's addressed by the general policy development and review requirements specified in 04.a, Information Security Policy Document, and 04.b, Review of the Information Security Policy. By addressing policy and process requirements in this way, the assessment can focus on more actionable requirements.

The implementation specifications for CSF control 01.a, level 1 can be used to further illustrate the approach:

> *Access control rules shall account for and reflect the organization's policies for information dissemination and authorization, and these rules shall be supported by formal procedures and clearly defined responsibilities. Access control rules and rights for each user or group of users shall be clearly stated in an access control policy. Access controls are both logical and physical and these shall be considered together. Users and service providers shall be given a clear statement of the business requirements to be met by access controls.*

Specifically, the policy shall take account of the following:

- *security requirements of individual business applications;*
- *policies for information dissemination and authorization (e.g., need-to-know, need to share, and least privilege principles; security levels; and classification of information.)*
- *relevant legislation and any contractual obligations regarding protection of access to data or services;*
- *standard user access profiles for common job roles in the organization;*
- *requirements for formal authorization of access requests;*
- *requirements for emergency access;*
- *requirements for periodic review of access controls; and*
- *removal of access rights.*

The organization shall develop, disseminate and review and update the access control policy and procedures annually.

HITRUST generated seven actionable requirements from this language (i.e., statements that do not specifically address policy or procedural requirements):

1. Access control rules and rights for each user or group of users are based on clearly defined requirements for information dissemination and authorization (e.g., need-to-know, need-to-share, least privilege, security levels and information classification).
2. Access control rules and rights for each user or group of users are clearly defined.
3. Users and service providers are given a clear statement of the business requirements (e.g., relevant legislation and any contractual obligations) to be met by access controls (i.e., to protect access to data or services).
4. The security requirements of individual business applications are defined.
5. The organization uses standard user access profiles for common job roles.
6. Requirements for formal authorization of access requests, emergency access, and the removal of access are defined.
7. The organization develops, disseminates, reviews, and updates the access control program annually.

These seven requirements were then condensed into the following three requirement statements for use in the MyCSF assessment and reporting tool.

1. Access control rules and rights for each user or group of users for each application are clearly defined in standard user access profiles (e.g., roles) based on need-to-know, need-to-share, least privilege, and other relevant requirements.
2. Users and service providers are given a clear statement of the business requirements for controls needed to protect access to data or services.
3. The access authorization process addresses requests for access, changes to access, removal of access, and emergency access.

During an assessment, an assessor would evaluate each of these three MyCSF requirement statements based on the organizational context provided by the general maturity requirements provided earlier in Table 1. The assessor would also use specific assessment guidance provided in MyCSF by the illustrative procedures specific to each requirement statement as well as specific criteria for the evaluation of each maturity level on a requirement statement by statement basis.

Using the Illustrative Procedures in MyCSF to Evaluate Requirement Statements

MyCSF provides illustrative procedures for each control requirement contained in an assessment. These procedures provide additional context for evaluation of these requirements and should be leveraged by assessors to help ensure consistency and repeatability of their control assessments.

Let's look at the procedures associated with the following level 1 requirement statement for CSF control 09.n, Security of Network Services:

> *Agreed services provided by a network service provider/manager are formally managed and monitored to ensure they are provided securely.*

The illustrative procedures associated with this requirement statement are as follows:

- **Policy:** *Examine policies and/or standards related to the management of network services and determine if the ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored, and the right to audit is agreed by management. The security arrangements necessary for particular services including security features, service levels, and management requirements, is identified and documented. If no written policy or standard exists, interview control owner(s) responsible for, key staff involved in/with, and/or other relevant stakeholders impacted by the policy/control requirement(s) and determine if the requirement(s) is/are understood. Evidence of ad hoc or informal policy may also be provided by observing individuals, systems and/or processes associated with the management of network services to determine if the policy requirements are generally understood and implemented consistently. Review any written procedure(s) or examine documentation associated with informal or ad hoc processes to determine if the requirement(s) is/are addressed consistently by the entity.*
- **Procedure:** *Determine if written procedures exist for management of network services and whether the procedure(s) address(es) each element of the policy/control requirement(s) stipulated in the policy level. Interview control owner(s) responsible for, key staff involved in/with, and/or other relevant stakeholders impacted by the policy/control requirements to determine if the procedure(s) address(es) all the required elements of the policy/control requirement(s) whether a written policy or procedure exists. Confirm their understanding of the procedure(s) as implemented and compare their understanding to any existing written procedure(s) to determine if they are consistent.*
- **Implemented:** *Examine relevant documentation, observe relevant processes, and/or interview the control owner(s), key staff, and/or relevant stakeholders, as needed, for the management of network services and determine if the policy/control requirements stipulated in the policy level have been implemented. For example, obtain a list of network service providers, including any internal network services provided locally or as an enterprise service, and compare the list to a list of network services agreements. Verify that each provider, including any internally provided services, has a network services agreement. Examine a representative sample of network services agreements and ensure they address the policy requirements for security, including the right to audit. If the original dates of the agreements can be determined, verify the network service agreements sampled were established prior to implementing/using the services. Ask if any of the service providers, including those provided by an internal network services manager, have been audited. Review documentation substantiating the audits. Review documentation substantiating the monitoring of these network services, including any actions taken to actively manage any security-relevant issues with the provided services.*
- **Measured:** *Examine measure(s) that evaluate(s) the organization's compliance with the third-party management policy and determine if the measure(s) address(es) implementation of the policy/control requirement(s) as stipulated in the policy level. For example, the measure(s) could indicate the number of network services that do not have a policy-compliant network services agreement as a % of all network*

services received. Non-compliance with the policy requirements could be part of a broader metric that considers all deviations from network services requirements regardless of type if non-compliance with the requirements for network services agreements can be ascertained. Reviews, tests, or audits should be completed by the organization to measure the effectiveness of the implemented controls and to confirm that agreed services provided by a network service provider/manager are formally managed and monitored to ensure they are provided securely. Note a broader or more general measure may be used if a root cause analysis or similar examination would indicate a deficiency in the stipulated policy/control requirements was the source of the observed deviation. A measure could also include regular or "ad hoc" reports or audits if it considers implementation of the appropriate policy/control requirement(s). If a metric adequately evaluates implementation of the policy/control requirement(s), also determine if the metric's frequency of observation (e.g., daily, weekly or monthly) and performance targets (e.g., above 99% or no more than 5%) are appropriate for the policy/control requirement(s).

- **Managed:** *Obtain and examine supporting documentation maintained as evidence of these metrics, measures, tests, or audits to determine if the office or individual responsible reviews the information and, if issues were identified, they were investigated and corrected. Determine if the individual or office can correct issues without the need to routinely escalate the issues to the next level of management. Note the ability to escalate issues must also exist if the root cause of a specific incident cannot be addressed by the individual or office receiving and reviewing the metric or measurement. Examine related records to determine if the individual or office conducted any follow-ups on the deviations to verify they were corrected as intended. If written records do not exist, interview personnel who receive and review the metric(s) to determine if ad hoc processes for investigation and resolution exist and if deviations occurred and were corrected.*

Internal and external assessors **MUST** use these procedures with the more general criteria (questions) and the scoring rubric provided for the maturity levels (discussed later in this document) to evaluate the level of compliance with each level for this requirement statement. For example, when reviewing the access control policy to evaluate compliance with level 1, Policy, does it provide language addressing defined requirements for standard access control profiles based on need-to-know, need-to-share, and least privilege, at a minimum? Does the policy cover all the organizational units and systems/assets in scope for the assessment? And has the policy been approved by management in accordance with organizational policy requirements and adequately communicated to the workforce?

Assessors should also note the general criteria and illustrative procedures, while intended to ensure a minimal level of rigor, consistency, and repeatability, are indeed illustrative but only in the sense that they provide a minimally acceptable standard of care. Assessors **MUST** use these criteria and procedures as the basis for more detailed assessment work plans, also known as security test and evaluation (ST&E) plans or simply test plans, which **MUST** also accompany any assessment submitted to HITRUST for quality assurance review in support of validation or certification.

Although requirement statements marked as N/A would not be evaluated (scored) during an assessment, assessors must provide the rationale for marking the requirement N/A in the requirement's comment field in the appropriate tab within the MyCSF tool.

Specific Criteria for Assessing Requirement Statements Against Each Level of the Maturity Model

The following table provides a minimum set of criteria in the form of questions based on the organizational-level criteria outlined earlier in Table 1Table 1. Organizational-level , which assessors must consider when evaluating a requirement statement at each level of the model. The criteria provide the necessary context for scoring against HITRUST's illustrative procedures.

Table 2. Requirement Statement-level Evaluation Criteria

Level	Requirement Statement-level Evaluation Criteria
1 - Policy	• Do formal, up-to-date policies or standards exist that contain "shall" or "will" statements for each element of the requirement statement? • Do the policies and standards that exist for each element of the requirement statement cover all major facilities and operations for the organizations and/or systems/assets in scope for the assessment? • Are the policies and standards that exist for each element of the requirement statement approved by management and communicated to the workforce?
2 - Procedure	• Do formal, up-to-date, documented procedures exist for the implementation of each element of the requirement statement? • Do the procedures clarify operational aspects such as how, when, who, and on what the action/control/requirement is to be performed? • Do the procedures outline stakeholder responsibilities? • Do the procedures address each element of the requirement statement across all applicable facilities, operations, and/or systems/assets in scope? • Are procedures for the implementation of each element of the requirements statement communicated to the individuals who are required to follow them? • Are the procedures approved by management?
3 - Implemented	• Is each element of the requirement statement implemented in a consistent manner everywhere that the policy and procedure apply, i.e., across the entire scope of applicable organizational and system elements, including the physical and logical systems used by a third-party that support the workflows for the products and/or services provided by the organization? • Are ad hoc approaches that tend to be applied on an individual or on a case-by-case basis discouraged?
4 – Measured	• Are self-assessments, audits, and/or tests routinely performed or other measures and/or metrics collected to evaluate the adequacy and effectiveness of the implementation of each element of the requirement statement? • Are evaluation requirements, including requirements regarding the type and frequency of self-assessments, audits, tests, and/or metrics collection documented, approved, and effectively implemented? • Does the frequency and rigor with which each element of the requirement statement is evaluated depend on the risks that will be posed if the implementation is not operating effectively? • Are measures supported by documentation that specifically addresses what is measured, who is responsible for gathering the data, how the data is recorded, how the measurement is performed/calculated, and how often the measurement is reviewed and by whom? • Do metrics meet all the requirements of a measure and also tracked over time and have explicitly stated (not implied), established thresholds (i.e., upper and/or lower bounds on a value) or targets (i.e., targeted goals, what the organization is trying to achieve)?
5 – Managed	• Is there a defined mechanism to track issues, risks, and risk treatment decisions? • Are effective corrective actions taken or other risk treatments applied to address identified weaknesses in the elements of the requirement statement, including those identified as a result of potential or actual information security incidents or through information security alerts? • Are measures and/or metrics provided to an appropriate level of management or, if not, is there a defined escalation or review process so that action may be taken by an appropriate level of management? • Do decisions around corrective actions consider cost, level of risk, and mission impact?

The HITRUST CSF control maturity model also incorporates the following 5-point compliance scale to rate each level in the model, as shown in Table 3.

Table 3. Maturity Model Compliance Scale

Score	Description
Non-Compliant (NC)	Very few if any of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured, or managed). Rough numeric equivalent of 0% (point estimate) or 0% to 10% (interval estimate).
Somewhat Compliant (SC)	Some of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured, or managed). Rough numeric equivalent of 25% (point estimate) or 11% to 32% (interval estimate).
Partially Compliant (PC)	About half of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).
Mostly Compliant (MC)	Many but not all of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured, or managed). Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).
Fully Compliant (FC)	Most if not all of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured, or managed). Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).

Ranges for the interval estimates are illustrative; assessor judgment should always be applied when determining the level of compliance with a specific requirement. The non-compliant and fully compliant ratings are relatively straight forward, but let's look at some examples of how the other three 'partial ratings' may be determined.

Suppose an organization has specified all the elements of a requirement statement in policy, but the policy only applies to three of the four business units within scope of the assessment. The organization would be mostly compliant (MC) for level 1, Policy. Now suppose that organization had written procedures supporting implementation of all the elements of the requirement statement across all four business units but only used/implemented these procedures in three of the four business units covered by the policy. The organization would be fully compliant (FC) for level 2, Procedures, and mostly compliant (MC) for level 3, Implementation.

For further illustration, let's examine one specific element, encryption, from a specific requirement statement for mobile computing devices derived from CSF control 01.x, Mobile Computing and Communications:

> *Mobile computing devices are protected at all times by access controls, usage restrictions, connection requirements, encryption, virus protections, host-based firewalls or equivalent functionality, secure configurations, and physical protections.*

The assessor has determined that the academic hospital in this scenario requires by policy, signed by executive management, that all portable computing devices—whether a laptop or a smartphone—be encrypted if the device is used to access covered information. The organization gets credit for full compliance with the encryption-related policy requirement. The organization has formal written procedures in place to ensure Windows-based laptops and all smartphones are encrypted according to the policy requirements but has yet to establish procedures for the encryption of a limited number of Mac laptops due to resistance from the research community. As it can demonstrate all Windows-based laptops and smartphones were encrypted when the

capability was rolled out earlier in the year, the hospital scores mostly compliant for encryption-related procedures and implementation.

The management console used by end-user devices and the mobile device management console for smartphones both have the capability to report on the encryption status for these devices and meet the requirements for an operational measure. Since manager bonuses are tied to meeting operational service levels, executive leadership lost interest once the encryption project was completed for Windows-based devices, which accounts for 95% of the total environment. The organization gets a somewhat compliant score for measured and noncompliance for managed, as the organization does not use this information to evaluate and manage the effectiveness of the encryption implementation.

Based on the facts presented, the scoring might look as follows for this requirement statement:

Table 4. Scoring Example

Level (Points)	NC	SC	PC	MC	FC
Policy (15)					X
Procedures (20)				X	
Implemented (40)				X	
Measured (10)		X			
Managed (15)	X				

The compliance scale is evenly weighted (0%, 25%, 50%, 75%, and 100%), but the PRISMA scores for each level are weighted differently (15 pts, 20 pts, 40 pts, 10 pts, and 15 pts).[xii] Essentially, the last two levels (measured and managed) are combined (for a total of 25 points) to address the concept of 'one can't manage what one can't measure' and still account for the fact that not all organizations actively manage their controls even while measuring their effectiveness. For example, an organization may perform a root cause analysis after every security incident but fail to take appropriate action based on the results.

In this example, the academic hospital would score the following for the encryption component of the requirement: (1)(15) + (.75)(20) + (.75)(40) + (.25)(10) + (0)(15) = 62.25. However, although this example focused on a specific element of the requirement statement, an assessor would likely not determine the state of compliance for any level of the model until all elements of the requirement were evaluated and could be aggregated to support a single score.

By way of another example using the first level, Policy, assume that requirements for access controls, encryption, virus protections, secure configuration, and physical protections are fully addressed by organizational policy. However, host-based firewalls are not. For this level, the state of compliance can be evaluated as (1+1+1+1+1+0) / 6 = 5/6 = 0.83, which is closest to Mostly Compliant, or MC. This exercise would then be repeated for the remaining four levels, after which an overall score for the requirement statement could be computed in the same manner as the encryption element described earlier.

Once all the elements of all the requirement statements are evaluated against HITRUST's PRISMA-based maturity model, the scores can be aggregated across all the requirement statements for a control or across multiple controls in a domain. These scores can also be used to support reporting against specific controls or

domains for one or more organizations, type(s) of business units across multiple organizations, one or more information systems, or type(s) of information systems.

Now let's consider two specific cases in which a specific technology is not implemented and illustrate how requirements associated with the technologies would be evaluated.

Suppose an organization prohibits the use of wireless access points in its environment. One might assume the assessor would indicate any CSF control requirements associated with this technology are not applicable and move on; however, this can't be done when the vulnerabilities associated with a technology like wireless could be introduced without the knowledge of the organization. As such, assessors should ask the following types of questions to evaluate the effectiveness of controls intended to ensure wireless access points are not procured or installed in violation of policy:

- **Policy:** Does the organization have a policy that states wireless access points are not allowed in any part of the environment within scope of the assessment?
- **Procedure:** Does the organization have processes in place to ensure that wireless access points are not procured or installed in any part of the environment within scope of the assessment, e.g., rogue wireless detection?
- **Implemented:** Does the organization check for wireless access points in all parts of the environment in scope for the assessment? Have these checks been accomplished at a frequency and manner (periodic and aperiodic/randomly) as required by policy?
- **Measured:** Does the organization track the results via some type of measurement?
- **Managed:** Does the organization have a process in place to report the measurement to management and take corrective action? In documented instances in which wireless access points have been detected, did the organization follow the process and take appropriate corrective action?

Note that the wireless scenario presented here indicates assessors cannot rely solely on illustrative procedures for the development of their test plans, which third-party assessors are required to submit to HITRUST as part of the validation and certification quality assurance process. An assessor would necessarily document alternate testing in the test plan similar to the language provided in the wireless scenario.

Let's look at another example. CSF control 01.b, User Registration states: "User identities are verified in person before a designated individual or office to receive a hardware token." How should an assessor evaluate this requirement if the organization does not use hardware tokens?

Unlike our wireless access point example, CSF control requirements associated with the use of this technology would truly be 'not applicable' or 'N/A' for this organization. The reason is this control addresses a risk that does not exist and will likely not exist given the very slim (virtually zero) likelihood the organization or individual (either well-meaning or malicious) would implement a rogue hardware token infrastructure. Basically, there's no need to have a policy restricting the use of hardware tokens or procedures in place to ensure hardware tokens aren't utilized. Scores for related requirement statements would not be calculated and subsequently not included in the scoring of any control, group of controls, or domain.

Leveraging the HITRUST CSF Scoring Rubric

Although the intent is for assessors to understand and apply these concepts to the scoring of each maturity level based on the organizational- and requirement statement-level criteria and requirement statement-specific illustrative procedures provided earlier in this document, HITRUST recognizes that internal (self) and external (third-party) assessors have various levels and types of experience upon which to base decisions. To help assessors score control maturity in a consistent and repeatable way, HITRUST developed a simple scoring rubric that could be used as an additional step in their evaluation of a requirement statement when they could not determine the state of compliance based on the previous guidance.

In the years since the simple scoring rubric was first published, it's become clear the rubric needed to be updated to better reflect the comprehensive approach HITRUST uses to evaluate control maturity and help ensure assessors are scoring a requirement statement's maturity levels accurately. The result is a greatly expanded rubric that addresses each of the five maturity levels in separate tables rather than the single table used previously. Developed by the HITRUST Offices of Compliance, Assurance, and Research & Analysis, the rubric has also been reviewed by various members of the HITRUST Assessor Council to help ensure usability in the field.

Rubric Structure

The five tables in the scoring rubric adhere to the structure depicted in Figure 1.

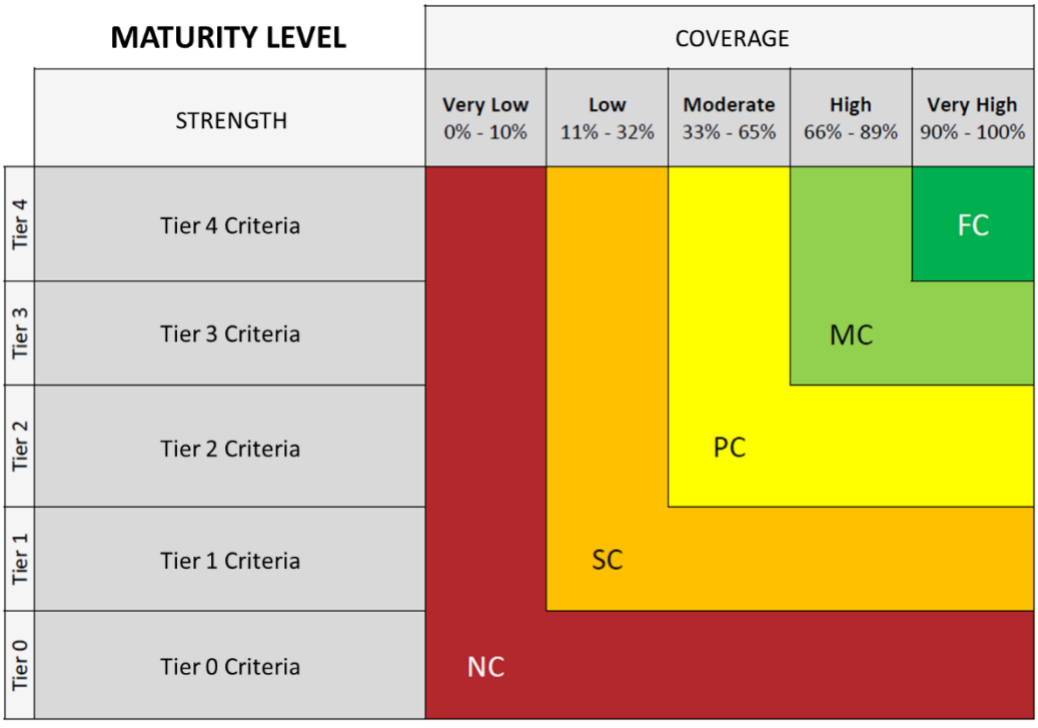


Figure 1. Rubric Template

The rows in the table, Tiers 0 through 4, represent increasing strength (rigor) in the maturity criteria. The columns, from very low to very high, represent the level of coverage (compliance) with respect to the elements specified for each requirement statement in the illustrative procedures for the evaluation of the maturity level.

It's also important to note that, although only specified explicitly in the Policy maturity level of the procedures, these elements apply to all five maturity levels in the model. The intersection of the level-specific strength and coverage result in one of five maturity ratings (NC, SC, PC, MC, or FC) from which the requirement's final maturity score is computed.

We'll use the following example to help illustrate application of the HITRUST CSF control maturity rubric. We identify this as 'Example 1' since three additional examples are provided in Appendix B – Additional Examples Using the Rubric.

Example 1 – Basic (Scenario)

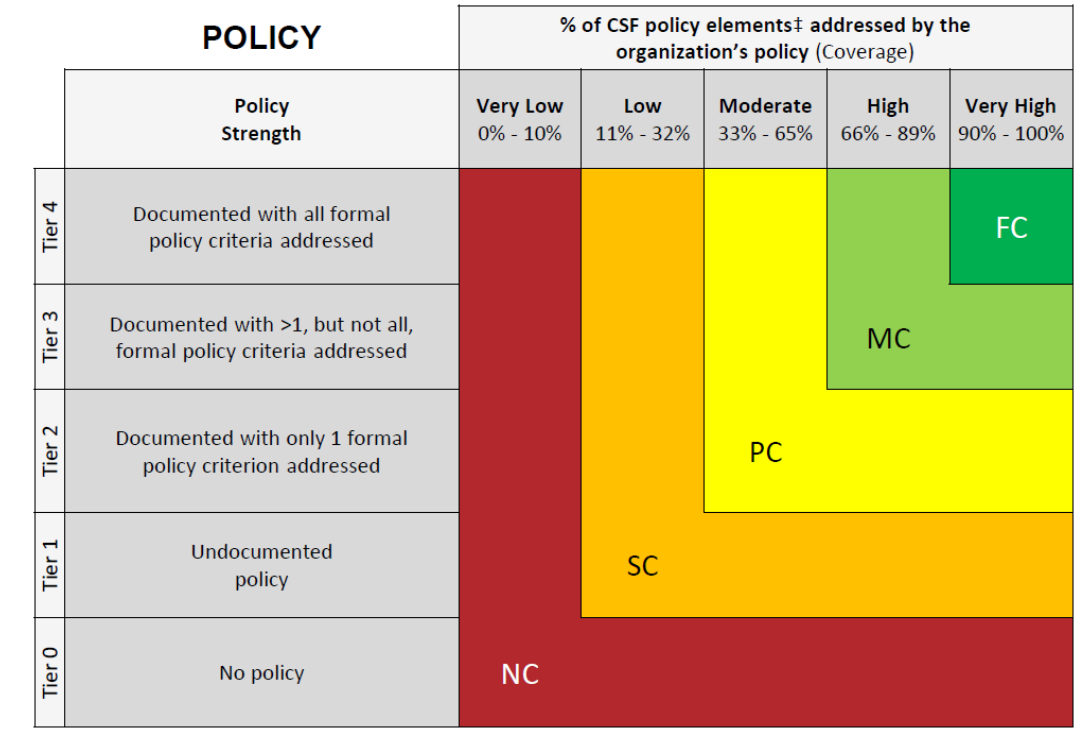
Consider an implementation specification from HITRUST CSF control 01.l, level 1, which states: *Access to network equipment shall be physical protected (e.g., a router must be stored in a room that is only accessible by authorized employees or contractors)*. The MyCSF requirement statement for this implementation specification has been shortened to:

Access to network equipment shall be physically protected.

We now present the table for each of the five maturity levels along with a discussion surrounding how the rubric for each level is applied to Example 1 for the first three levels: policy, procedure, and implemented.

Policy

The table for the *Policy* maturity level is provided in Figure 2.



‡ As specified in the policy level's illustrative procedure in MyCSF

Figure 2. Policy Rubric

The criteria help indicate the strength of the policy and include the following:

- The policy is (or policies are) demonstrably approved by management,
- The policy is (or policies are) demonstrably communicated to stakeholders in the organization and members of the workforce, and
- The policy (or policies) clearly communicate(s) management's expectations of the control's operation (e.g., using "shall", "will", or "must" statements).

Example 1 – Basic (Policy)

To facilitate the assessment process, relevant elements of the HITRUST CSF control implementation specifications are provided in the MyCSF requirement statement's illustrative procedures for the Policy maturity level, which obviates the need for assessors to refer back to the original CSF control language unless they need additional context for the requirement.

The illustrative procedure for Policy explains that assessors should examine policies and/or standards related to the physical protection of network equipment and determine if access to network equipment is physically protected (e.g., a router must be stored in a room that is only accessible by authorized employees or contractors).

Because this requirement focuses on access to networking equipment, all networking equipment within scope of the assessment are relevant. If this was a logical access test, it's likely the population of all systems in scope for the assessment would be considered instead. Also, because there's only one CSF requirement statement element in this example, i.e., network devices must be physically protected, policy coverage is either 0% (VL) or 100% (VH). Again, this is a basic example; not all requirement statements have only one CSF policy element.

The steps need to assess the maturity of this requirement at the policy level include:

- Step 1 – Identify relevant policies (even unwritten ones)
- Step 2 – Review the policies to determine coverage relevant to the requirement's elements
- Step 3 – Review the policies to determine strength relevant to the policy criteria
- Step 4 – 'Plug' what you've learned into the policy rubric to determine the maturity rating

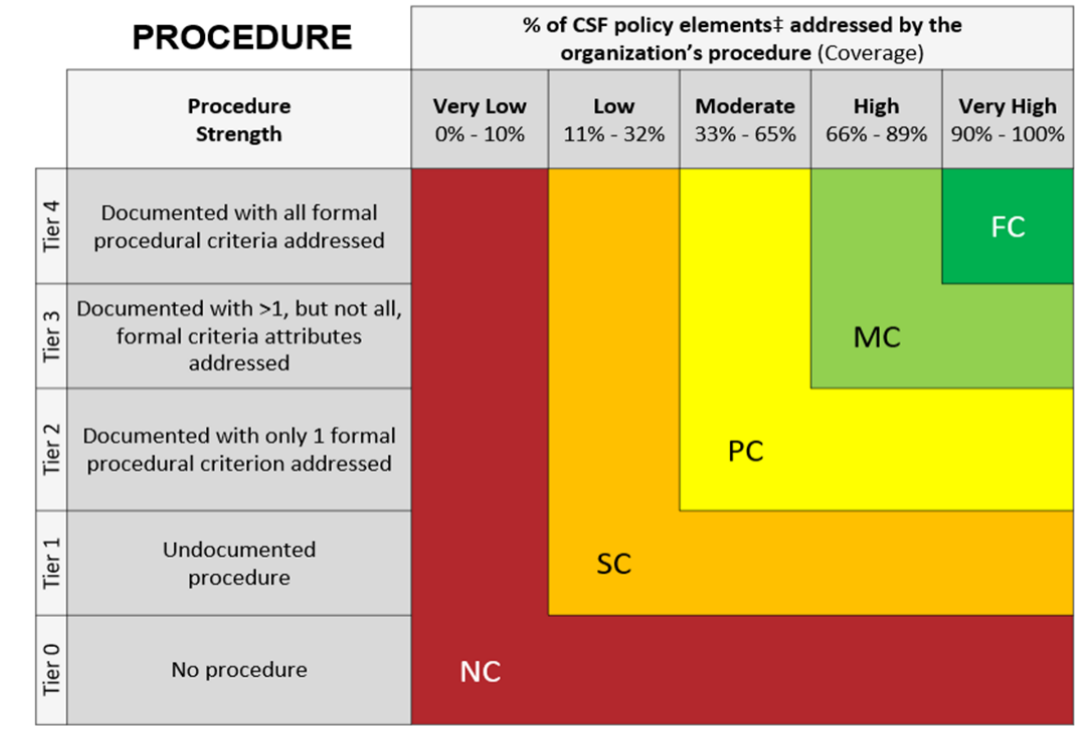
Table 5 provides the results for five different scenarios using the policy rubric.

Table 5. Example 1 Assessment Results - Policy

Assessment Results	Policy Strength	Policy Coverage	Policy Level Rating
No policy	Tier 0	VL (0%)	NC
An undocumented policy only	Tier 1	VH (100%)	SC
A written policy that spells out expectations but has never been approved or communicated	Tier 2	VH (100%)	PC
An approved written policy that spells out expectations but has never been communicated	Tier 3	VH (100%)	MC
An approved, communicated, written policy that spells out expectations	Tier 4	VH (100%)	FC

Procedure

The table for the *Procedure* maturity level is provided in Figure 3.



‡ As specified in the policy level's illustrative procedure in MyCSF

Figure 3. Procedure Rubric

The criteria around procedural documentation help indicate the strength of the procedure(s) and include the following:

- The procedure(s) is/are demonstrably approved by management,
- The procedure(s) is/are demonstrably communicated to stakeholders,
- The procedure(s) outlines stakeholder responsibilities, and
- The procedure(s) discuss(es) operational aspects such as how, when, who, and on what the action / control / requirement is to be performed.

Example 1 – Basic (Procedure)

Continuing our example around the physical protection of network devices, the steps needed to assess the maturity of this requirement for the procedure level include:

- Step 1 – Identify relevant procedure(s) (even unwritten ones)
- Step 2 – Review the procedure(s) to determine coverage relevant to the requirement's elements
- Step 3 – Review the procedure(s) to determine strength relevant to the scope of the procedural criteria
- Step 4 – 'Plug' what you've learned into the procedure rubric to determine the maturity rating

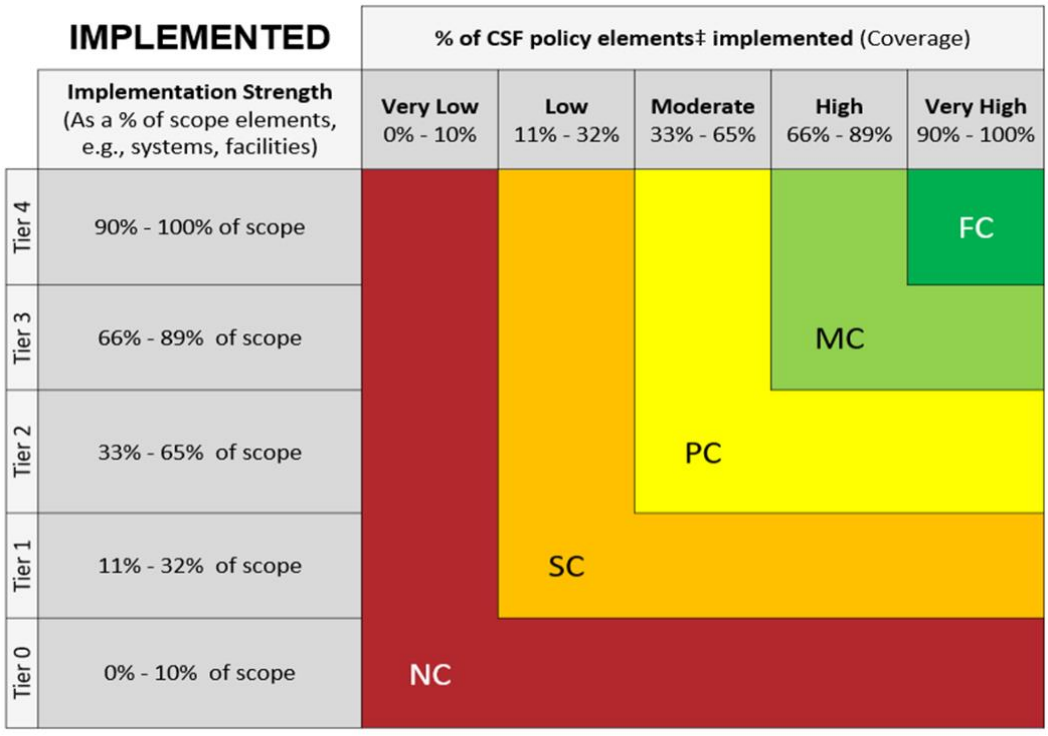
Table 6 on the following page provides the results for five different scenarios using the procedure rubric.

Table 6. Example 1 Assessment Results - Procedure

Assessment Results	Procedure Strength	Procedure Coverage	Procedure Level Rating
No procedure	Tier 0	VL (0%)	NC
An undocumented procedure only	Tier 1	VH (100%)	SC
A written procedure that discusses all operational aspects but has not been approved or communicated	Tier 2	VH (100%)	PC
An approved written procedure discusses all operational aspects but has not been communicated	Tier 3	VH (100%)	MC
An approved, communicated, written procedure discusses all operational aspects	Tier 4	VH (100%)	FC

Implemented

The table for the *Implemented* maturity level is provided in Figure 4.



‡ As specified in the policy level's illustrative procedure in MyCSF

Figure 4. Implemented Rubric

The control's implementation strength is evaluated by considering the control's application across the assessment scope, which consists of all applicable organizational and system elements and includes the physical and logical systems used by a third party that support the workflow(s) for the product(s) and/or service(s) provided by the organization, as well as the logical interfaces to the systems included in the assessment scope.

Example 1 – Basic (Implemented)

Continuing our example around the physical protection of network devices, we'll need to determine the strength of the implementation by identifying how many of the in-scope systems and/or organizational elements have the CSF requirements implemented as specified by policy. For example, if there are four networking devices in scope and all were physically protected, this would indicate a strength of Tier 4. If only three of four devices were protected, this would indicate a strength of Tier 3.

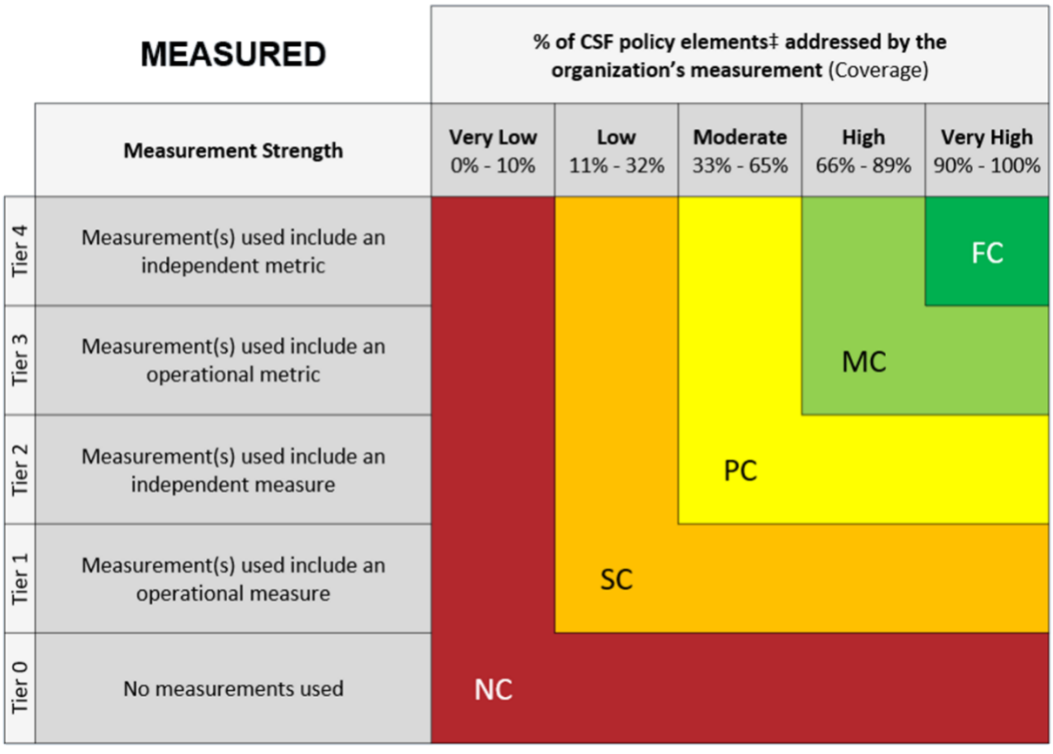
Table 7Table 1 provides the results for five different scenarios using the rubric.

Table 7. Example 1 Assessment Results - Implemented

Assessment Results	Implementation Strength	Implementation Coverage	Implemented Level Rating
0 of 4 devices (0%) are physically protected	Tier 0	VL (0%)	NC
1 of 4 devices (25%) are physically protected	Tier 1	VH (100%)	SC
2 of 4 devices (50%) are physically protected	Tier 2	VH (100%)	PC
3 of 4 devices (75%) are physically protected	Tier 3	VH (100%)	MC
4 of 4 devices (100%) are physically protected	Tier 4	VH (100%)	FC

Measured

The table for the *Measured* maturity level is provided in Figure 5.



‡ As specified in the policy level's illustrative procedure in MyCSF

Figure 5. Measured Rubric

The criteria for strength of the measurement used by an organization includes whether:

- The measurement should be considered a measure or a metric, and
- The measurement is obtained by the control owner, i.e., operationally, or if it is obtained independently of the control owner.

A measure is a mechanism used to formally evaluate and communicate the operation/performance of an implemented control or requirement. Measures are measurements that are prepared in real-time or at a set cadence (e.g., weekly, monthly, quarterly, annually) using a defined set of inputs (e.g., system-generated reports) by an understood/clearly defined owner.

To be classified a measure for HITRUST CSF Assessment purposes, it must (1) address the control's operation/performance, (2) be used at an appropriate frequency, and (3) be supported by documentation that addresses specifically:

- What is measured,
- Who is responsible for gathering the data,
- How the data is recorded,
- How the measurement is performed/calculated, and
- How often the measurement is reviewed and by whom.

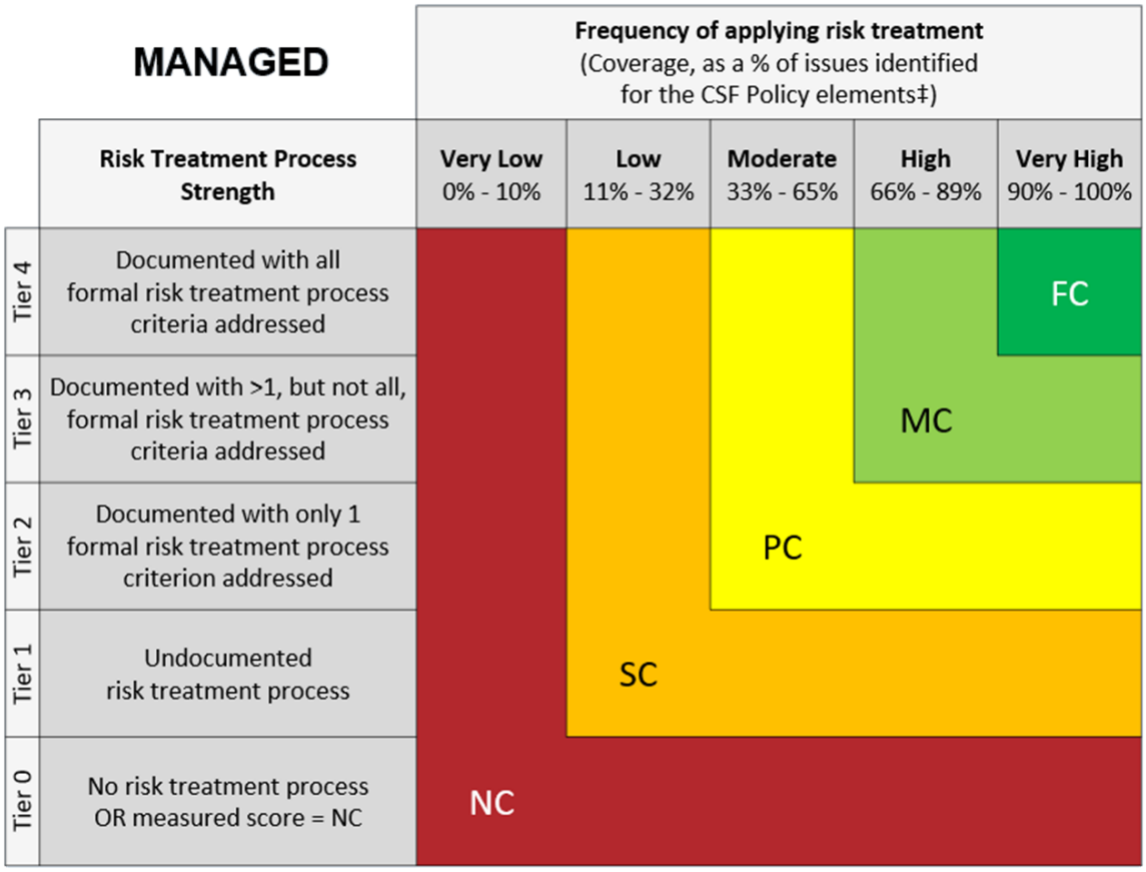
To be classified as metric for HITRUST CSF Assessment purposes, the measurement must meet ALL requirements for a measure (listed above) AND:

- Be tracked over time, and
- Have explicitly stated (not implied), established thresholds (i.e., upper and/or lower bounds on a value) or targets (i.e., targeted goals, what the organization is trying to achieve).

In general, "measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline of two or more measurements taken over time"[xiii] and generally include a value to be achieved or avoided (or both).

Managed

The table for the *Managed* maturity level is provided in Figure 6 on the following page.



‡ As specified in the policy level's illustrative procedure in MyCSF

Figure 6. Managed Rubric

The criteria for management (against relevant measures and/or metrics) center around the strength of the documented risk treatment process and include:

- Initial involvement of an appropriate level of management or a defined escalation or review process to be observed if/when the appropriate level of management is not initially involved,
- A defined mechanism to track issues, risks, and risk treatment decisions, and
- Whether cost, level of risk, and mission impact are considered in risk treatment decisions.

A copy of the most current version of the HITRUST CSF control maturity scoring rubric can be downloaded from the HITRUST website's download page for CSF Assurance & Related Programs.

Final Thoughts

If properly followed, HITRUST's Risk Management Framework (RMF) provides the structure and rigor needed to ensure consistent and repeatable assessments that provide reliable assurances to organizational and external stakeholders. However, the rigor of these structured assessments may be somewhat new to many entities and assessor organizations.

Assessors cannot rely solely on prior experience with PCI, AICPA, or other security and privacy assessment methodologies to provide a HITRUST CSF Assessment. HITRUST organizations and assessors should ensure they understand the HITRUST RMF, CSF Assurance Program requirements, and the CSF assessment process outlined in the CSF Assessment Methodology. Only then can one thoroughly understand how to evaluate HITRUST CSF controls using the HITRUST maturity model, evaluation, and scoring approach, and the use of organizational- and requirement statement-level criteria and requirement statement-specific illustrative procedures to build out the test plans needed to conduct a successful CSF assessment.

The provision of a new, more comprehensive maturity scoring rubric that better integrates the evaluation guidance for HITRUST CSF controls will ensure internal and external assessors apply the guidance appropriately and improve internal and external consistency of maturity ratings and scores.

To understand how the HITRUST RMF is used by healthcare organizations to implement the NIST *Framework for Improving Critical Infrastructure Cybersecurity*,[xiv] more commonly known as the NIST Cybersecurity Framework, see the *Healthcare Sector Cybersecurity Framework Implementation Guide*,[xv] available on the US-CERT Cybersecurity Framework Website.[xvi]

About HITRUST

Founded in 2007, HITRUST Alliance is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security, and risk management leaders from both the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management and de-identification frameworks; related assessment and assurance methodologies; and initiatives advancing cyber sharing, analysis and resilience, all of which comprise the HITRUST Approach to a comprehensive information security and privacy risk and compliance management ecosystem.

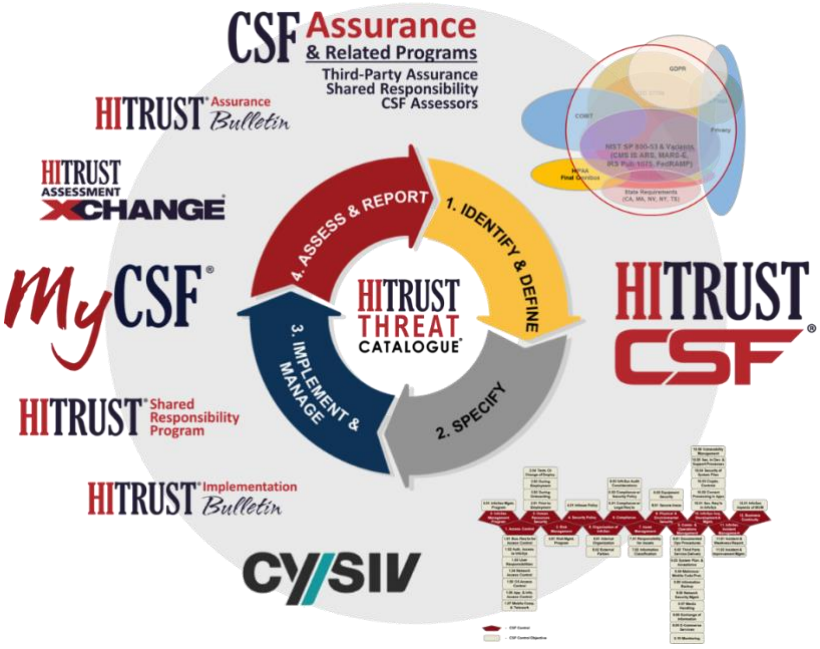


Figure 7. The HITRUST Approach

HITRUST also actively participates in many efforts in government advocacy, community building, and cybersecurity education. For more information, visit www.hitrustalliance.net.

About the Authors

Bryan Cline, Ph.D., Chief Research Officer

Bryan provides thought leadership on risk management and compliance and develops the methodologies used in various components of the HITRUST Approach. This includes a focus on the design of the HITRUST CSF and the assessment and certification models used in the HITRUST CSF Assurance Programs, for which he provides technical direction and oversight. He's also responsible for addressing emerging trends impacting risk management and compliance to ensure the HITRUST Approach sets the bar for organizations seeking the most comprehensive privacy and security frameworks available. Bryan previously served as HITRUST's Vice President of Standards and Analysis.

Jeremy Huval, VP, Compliance

Jeremy ensures the integrity of the HITRUST CSF Assurance Program. He and his team conduct quality reviews on all certified reports issued by HITRUST and continue to collaborate with the HITRUST Assurance team on matters such as report generation, process optimization, HITRUST CSF Assurance Program Requirements updates, and MyCSF enhancements. Jeremy also leads HITRUST's Internal Audit Department, an internal consulting and assurance function aimed at improving internal operations and ensuring an appropriate level of internal controls exist within the organization.

Bimal Sheth, VP, Assurance Services

Bimal leads the HITRUST Assurance Program; his team is responsible for ensuring the integrity of the HITRUST Certification program through quality assurance reviews of all submitted assessments and the production of final reports as well as deploying training for the CCSFP Certification. He is also responsible for communicating with assessors and customers during the quality assurance process and works closely with the Compliance team to design, develop, and implement new solutions to optimize the quality assurance process.

Appendix A – Glossary of Terms

Assurance Grounds for justified confidence that a claim has been or will be achieved. Note 1: Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated. Note 2: Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims. [NIST Glossary]

Automated Controls Controls that have been programmed, configured, and/or embedded within a system. [Adapted from the ISACA Glossary]

Automated controls are performed by systems—not people—based on configurations, rulesets, or programming. An example of an automated control is forced password expiration after the number of days specified in the associated configuration. [HITRUST]

Compliance An adherence to the laws, regulations, standards, guidelines, and other specifications [such as contractual obligations] relevant to an organization's business. For more information on compliance and compliance-related risk, see the HITRUST Risk vs. Compliance Whitepaper, p. 3.

Data Information in a specific representation, usually as a sequence of symbols that have meaning [or] pieces of information from which 'understandable information' is derived. [NIST Glossary]

Diligence Earnest and persistent application of effort especially as required by law. [FindLaw Dictionary]

Due Care The care that an ordinarily reasonable and prudent person would use under the same or similar circumstances; also called ordinary care or reasonable care. [FindLaw Dictionary]

Due Diligence Such diligence as a reasonable person under the same circumstances would use; use of reasonable but not necessarily exhaustive efforts; also called reasonable diligence. [FindLaw Dictionary]

Independent Measurement Independent measures and metrics are prepared by a person or group (e.g., auditors, analysts) who are not influenced by the person or group responsible for the operation of the requirement/control being measured (e.g., the control owner). [HITRUST]

Information Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. [NIST Glossary] Not to be confused with the term 'data.'

Measure(s) The results of data collection, analysis, and reporting. [NIST Glossary]

A standard used to evaluate and communicate performance against expected results (measures are normally quantitative in nature capturing numbers, dollars, percentages, etc., but can also address qualitative information such as customer satisfaction; reporting and monitoring measures help an organization gauge progress toward effective implementation of strategy). [ISACA Glossary]

Measurement The process of data collection, analysis, and reporting. [NIST CSRC Glossary]

Measurements are "observations that quantitatively reduce uncertainty." [Hubbard, D., Seiersen, R., Geer Jr., D., and McClure, S. (2016). How to Measure Anything in Cybersecurity Risk. John Wiley & Sons]

Metric(s) Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. [NIST Glossary]

A quantifiable entity that allows the measurement of the achievement of a process goal (metrics should be SMART—specific, measurable, actionable, relevant, and timely; complete metric guidance defines the unit used, measurement frequency, ideal target value, if appropriate, and also the procedure to carry out the measurement and the procedure for the interpretation of the assessment). [ISACA Glossary]

Natural Person A human being as distinguished from a person (as a corporation) created by operation of law. [GDPR Art. 4]

Operational Measurement Operational measures and metrics are prepared by a person or group responsible for the control/requirement being measured (e.g., the control owner) or by a person or group influenced by the control owner (a subordinate, a peer reporting to the same department head, etc.). [HITRUST]

Personal Data Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person. [GDPR Art. 4]

Policy Overall intention and direction as formally expressed by management, most often articulated in documents that record high-level principles or course of actions; the intended purpose is to influence and guide both present and future decision making to be in line with the philosophy, objectives, and strategic plans established by the enterprise's management teams. [Adapted from the ISACA Glossary]

Procedure A detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes. [Adapted from the ISACA Glossary]

Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Information-related] … risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, [and] other organizations…. [Adapted from the NIST Glossary]
Risk Management	The program and supporting processes to manage information security risk … and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time. [Adapted from the NIST Glossary]
Risk Treatment	Selecting and implementing mechanisms to modify risk. Risk treatment options can include avoiding, optimizing, transferring, or retaining [accepting] risk. [ENISA Glossary]
Rubric	An evaluation tool or set of guidelines to facilitate measurement against a consistent set of criteria. [Adapted from the Glossary of Education Reform.]
Sensitive Information	Information where the loss, misuse, or unauthorized access or modification could adversely affect the [organization] or the conduct of [organizational] programs [or services], or the privacy to which individuals are entitled [by law]. [Adapted from the NIST Glossary]
Standard of Care	The degree of care or competence that one is expected to exercise in a particular circumstance or role. [FindLaw Dictionary]
Undocumented	Not supported by written proof. [Cambridge Dictionary]

Appendix B – Additional Examples Using the Rubric

Example 2 – Applicability

Scenario

In this example we'll score all 5 HITRUST CSF control maturity levels for this HITRUST CSF requirement statement:

> *If it is determined that encryption is not reasonable and appropriate, the organization documents its rationale and acceptance of risk.*

This requirement statement comes from HITRUST CSF control 01.x, which has identical language, and its evaluation is generally straightforward. However, this type of requirement may not always be applicable to the organization.

To better understand the context for evaluating a requirement statement, HITRUST recommends referring to the language surrounding the requirement (if not the control's specification or overarching control objective). In this case, HITRUST CSF control 01.x states:

> *The organization shall use full-disk encryption to protect the confidentiality of information on laptops and other mobile devices that support full-disk encryption. Encryption shall be required for all other mobile computing devices in accordance with the organization's data protection policy (see 06.d) and enforced through technical controls. If it is determined that encryption is not reasonable and appropriate, the organization shall document its rationale and acceptance of risk.*

We see that this requirement applies to full-disk encryption of "laptops and other mobile devices" that support it and such encryption must be "in accordance with the organization's data protection policy [as required by CSF control 06.d] and enforced through technical controls." This would indicate the assessor should ensure any exception to policy for this encryption requirement consider these factors.

Evaluation

Let's assume the assessor performed the required fieldwork and during the walkthroughs learned from management that all sensitive data shall be encrypted at rest and in motion and that all mobile devices shall be encrypted without exception. This is further substantiated by a formal policy that states the same requirement.

Policy. The policy meets all of HITRUST's formal policy criteria on encryption (reference the contextual language provided in the HITRUST CSF control), even though there is no written policy that discusses documenting rationale for not encrypting or accepting the risk of not encrypting as no exceptions are allowed.

Because sensitive data must always be encrypted (without exception), the assessor should therefore mark this requirement as 'not applicable' (N/A for all five maturity levels).

Example 3 – Interpretation

Scenario

This example is similar to Example 2 as it uses the same HITRUST CSF requirement statement:

> *If it is determined that encryption is not reasonable and appropriate, the organization documents its rationale and acceptance of risk.*

As stated previously, this requirement statement comes from HITRUST CSF control 01.x, which has identical language, and applies to full-disk encryption of "laptops and other mobile devices" that support it and such encryption must be "in accordance with the organization's data protection policy [as required by CSF control 06.d] and enforced through technical controls." Again, this would indicate the assessor should ensure any exception to policy for this encryption requirement consider these factors.

However, unlike Example 2, the assessor determined the organization appears to allow exceptions to the encryption policy, which means this requirement cannot be marked N/A and must be evaluated on its face.

Evaluation

Policy. A "Mobile Device Policies and Procedures" document states, "All PHI, PII, and sensitive data shall be encrypted," and also states, "All mobile devices, laptops, smartphones, and other portable media shall be encrypted." The policy meets all of HITRUST's formal policy criteria. However, no policy exists in writing which discusses documenting rationale for not encrypting or accepting the risk of not encrypting.

Policy should be scored as non-compliant (NC). While the policy does talk about encrypting mobile devices, encrypting mobile devices isn't the focus of this requirement statement. Instead, this requirement is about the risk acceptance process for mobile devices that are not encrypted (a topic that this policy fails to address).

Procedure. The "Mobile Device Policies and Procedures" document doesn't actually contain any procedures (despite the name). It only contains policy statements which feature "shall", "will", and "must" language. The assessor's inquiries of various members of the workforce showed that no consensus exists on what to do if and when it is determined encrypting a mobile device is not reasonable and appropriate.

Procedure should be scored as non-compliant (NC) since procedures do not exist.

Implemented. Comparison of a system-generated population of mobile devices (including laptops and phones) against the IT asset inventory (deemed complete through the testing of another requirement statement) showed that 75% of the organization's mobile devices are encrypted. However, the organization has not documented the rationale for its failure to encrypt the remaining 25% of its mobile devices.

Implemented should be scored as non-compliant (NC); 75% of devices were encrypted, encryption coverage is tested via a separate requirement statement. This requirement is about the risk acceptance process for unencrypted mobile devices, which is not addressed.

Measured. Management doesn't claim it collects measures or metrics for its controls.

Measured should be scored as non-compliant (NC).

Managed. Management doesn't claim it manages its controls based on measures or metrics.

Managed should be scored as non-compliant (NC).

Example 4 – Varied Strength and Coverage

Scenario

In this example we'll score all 5 PRISMA levels for this one HITRUST CSF requirement statement:

> *Fire extinguishers and detectors are installed according to applicable laws and regulations.*

This requirement statement comes from HITRUST CSF control 08.d, which has more detailed language than the requirement statement:

> *The following controls shall be implemented to avoid damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster:*
>
> 1. *Appropriate fire extinguishers shall be located throughout the facility, and shall be no more than fifty (50) feet away from critical electrical components; and*
> 2. *Fire detectors (e.g., smoke or heat activated) shall be installed on and in the ceilings and floors.*

Subsequently evaluation of the requirement is not as straightforward as our earlier examples and must account for potential variations in strength and coverage of the various elements of the requirement.

(We note again the additional specificity around relevant elements of a requirement statement will always be provided in the statement's illustrative procedure for the policy maturity level. This obviates the need for assessors to refer to the HITRUST CSF unless additional context for the requirement statement is needed, e.g., to view additional language for the control or ascertain the control's specification or overarching objective.)

The scope for this assessment includes corporate offices ("Office"), and two 20' x 20' data centers ("DC1" and "DC2")

Evaluation

Policy. The entity has a "Data Center Environmental Protections Policy" which meets all of HITRUST's formal policy criteria, but this policy is only applicable to data centers (not office buildings). The Data Center Environmental Protections Policy states, "Clearly marked fire extinguishers must be placed near each entry and exit." There is no mention of fire detectors and no further mention of placement of fire extinguishers relative to critical electronics. However, the small size of the data centers makes it impossible for a fire extinguisher to be more than 50' from any electronic equipment. Further, no policies exist addressing environmental protections in corporate offices, which is unsurprising given no fire protections were noted during an office tour.

To further evaluate this requirement for the policy level, one must determine the number of policy elements in the policy illustrative procedure. There are 4 in this example:

(1) Fire extinguishers are located throughout the facility,
(2) Fire extinguishers are located… no more than 50' away from critical electrical components,
(3) Fire detectors are installed on and in… ceilings, and
(4) Fire detectors are installed on and in… floors.

Because the Data Center Environmental Protections Policy meets all of HITRUST's formal policy criteria, we know it has a Tier 4 strength.

Coverage is then determined by evaluating each element of the requirement individually, as shown in Table 8.

Table 8. Example 4 Assessment Results for Coverage – Policy

Element of the Requirement	Office	DC1	DC2
Fire extinguishers throughout	Not Covered	Covered	Covered
Fire extinguishers ≤ 50’	Not Covered	Covered	Covered
Fire detectors in ceilings	Not Covered	Not Covered	Not Covered
Fire detectors in floors	Not Covered	Not Covered	Not Covered
Coverage	**0%**	**50%**	**50%**

A simple average of the scores indicates overall coverage of the elements is 33.3%, or on the low-end of moderate, and policy should subsequently be scored as PC since strength is evaluated at Tier 4.

Procedure. For the two data centers, the assessed entity has a written “Data Center Fire Protections Procedure” addressing operational aspects of use, placement, and maintenance of fire extinguishers and clearly lays out stakeholder responsibilities. However, the entity couldn't demonstrate to the assessor this procedure had been formally approved or communicated. Further, no policies exist addressing environmental protections in corporate offices, which the assessor found unsurprising given no fire protections were noted.

Table 9 provides the assessor’s evaluation of the procedure’s strength relative to the criteria.

Table 9. Example 4 Assessment Results for Criteria – Procedure

Criteria	DC2
Demonstrably approved by management	Not Met
Demonstrably communicated to stakeholders	Not Met
Outlines stakeholder responsibilities	Met
Discusses operational aspects such as who, what, when, where, and how	Met
% of Criteria Addressed	**50%**

As the procedure is formally documented and 50% of the procedure criteria have been met, the procedure strength is evaluated as Tier 3.

Table 10 provides the assessor’s evaluation of the procedure’s coverage relative to the scope of the assessment.

Table 10. Example 4 Assessment Results for Coverage – Procedure

Element of the Requirement	Office	DC1	DC2
Fire extinguishers throughout	Not Covered	Covered	Covered
Fire extinguishers ≤ 50’	Not Covered	Covered	Covered
Fire detectors in ceilings	Not Covered	Not Covered	Not Covered

Fire detectors in floors	Not Covered	Not Covered	Not Covered
Coverage	**0%**	**50%**	**50%**

A simple average of the scores indicates overall coverage of the elements is 33.3%, or on the low-end of moderate, and procedure should subsequently be scored as PC since strength is evaluated at Tier 3.

Implemented. During an office tour the assessor noted that no fire extinguishers or detectors were present. A DC1 tour revealed that fire extinguishers are present and that fire detectors aren't installed. And a DC2 tour yielded no exceptions. All policy elements were met.

The maturity rating can be readily computed by leveraging a single table for coverage since there are no other criteria for implementation similar to policy and procedure, and 100% of the scope was assessed. Implementation of the requirement statement is reflected in Table 11.

Table 11. Example 4 Assessment Results for Coverage – Implemented

Element of the Requirement	Office	DC1	DC2
Fire extinguishers throughout	Not Implemented	Implemented	Implemented
Fire extinguishers ≤ 50’	Not Implemented	Implemented	Implemented
Fire detectors in ceilings	Not Implemented	Not Implemented	Implemented
Fire detectors in floors	Not Implemented	Not Implemented	Implemented
Coverage	**0%**	**50%**	**100%**

A simple average yields (0% + 50% +100%)/3 or 50%, and policy should subsequently be scored as PC.

Measured. Internal Audit or “IA” (which is in no way tied to the operation of this requirement) tests that fire extinguishers at the DC’s exist and are maintained on an annual basis. IA's test documentation contains details of who tested, what was tested, when testing happened, how the test was performed, and the result. IA also has a written procedure on communicating audit findings to executive management, which is always observed. However, IA doesn't include any comparison of testing results across time periods and doesn't identify any thresholds or performance targets.

Table 12 provides the assessor’s evaluation of the procedure’s strength relative to the criteria.

Table 12. Example 4 Assessment Results for Criteria – Measured

Criteria	DC2
Addresses the control’s operation/performance	Met
Used at an appropriate frequency	Met
Is supported by documentation that addresses the criteria for a measure, i.e., what is measured, who is responsible for gathering the data, how the data is recorded, how the measurement is performed/calculated, and how often the measure is reviewed and by whom.	Met

Meets the criteria for a measure, is tracked over time, and includes performance targets and/or a minimum or maximum threshold	Not Met
% of Criteria Addressed	**50%**

Note the requirements for a measure and a metric, as outlined in the last two rows in the table (prior to the '% of Criteria Addressed'), are 'all or nothing.' A measurement must meet all the relevant criteria for it to be considered a measure or metric. Note also that a measurement cannot be a metric if it does not meet the criteria for a measure.

As the measurement meets all the criteria for the measured maturity level except for those specified for a metric and is considered an independent measurement, measurement strength can be evaluated as Tier 2 (i.e., independent measure).

Table 13 provides the assessor's evaluation of the measurement relative to the scope of the assessment.

Table 13. Example 4 Assessment Results for Coverage – Measured

Element of the Requirement	Office	DC1	DC2
Fire extinguishers throughout	Not Measured	Measured	Measured
Fire extinguishers ≤ 50'	Not Measured	Measured	Measured
Fire detectors in ceilings	Not Measured	Not Measured	Not Measured
Fire detectors in floors	Not Measured	Not Measured	Not Measured
Coverage	**0%**	**50%**	**50%**

A simple average of the scores indicates overall coverage of the elements is 33.3%, or on the low-end of moderate, and measured should subsequently be scored as PC since strength is evaluated at Tier 3.

Managed. Executive management reviews all of IA's audit reports but doesn't always act when findings are noted. Fire extinguisher findings are rarely subject to any risk treatment (about 5% of the time if that). No formal risk treatment process exists.

Managed is subsequently scored as NC.

Appendix C – Frequently Asked Questions (FAQs)

1. **Can you provide an example for which an assessed entity might score near the top left of a rubric table (e.g., Tier 4 strength with very low coverage)?**

   Suppose an assessor determines management is using an independent metric to monitor performance of a given HITRUST CSF requirement statement. Review of the metric's documentation verifies management's assertion as (i) all of HITRUST's formal metrics criteria are in place, (ii) management tracks the results of the metric over time to identify variances and patterns, (iii) the metric is produced by a party independent of the control's operation, and (iv) performance targets are clearly defined. As such, the assessor agrees this the measurement has a strength of Tier 4 (independent metric). However, the assessor discovers the measurement doesn't address the bulk of the requirement's elements, which results in very low coverage. In this case the independent metric doesn't fit well with the requirement and subsequently fails to adequately monitor the control.

2. **Can you provide an example for which an assessed entity might score near the bottom right of a rubric table (e.g., Tier 0 strength with very high coverage)?**

   Let's look at a specific HITRUST CSF requirement statement: *Scans for malicious software are performed on boot and every 12 hours*. Let's assume that 50 laptops and 50 desktops make up the assessment's in-scope endpoint population. The illustrative procedure for policy shows the requirement statement does not have any additional elements, i.e., the only two elements that need to be assessed or (i) malware scans are performed on boot and (ii) every 12 hours. The assessor determines the organization's centrally managed anti-malware software is configured to force managed endpoints to scan on boot and every 12 hours. As such, 100% of the requirement statement's elements are met (very high coverage). However, the assessor's testing procedures revealed that only 9 of the 100 in-scope endpoints have the managed anti-malware client installed. As such, the strength is very low at 9%.

3. **How might a written procedure differ for an automated control vs. a manual control?**

   Several differences between written procedures for automated controls vs. manual controls are outlined in the Table 14 below.

Table 14. Differences in Documentation for Automated and Manual Controls

Characteristic	Manual Control Procedures	Automated Control Procedures
Primary audience	Various individual(s) across the organization may be responsible for performing the control	System Administrators are generally responsible for performing the control
Content	Addresses operational aspects of performing the control such as who, what, when, where, and how	A discussion of how the system should behave (through configuration settings or through programming) in order to consistently perform the control (and may include such things as screenshots)
Approach	"Here's how you as the control owner should do X."	"Here's how you as the system administrator should instruct the system to do X."

4. What does it mean to "decompose scope" and why use the word "decompose" in the guidance?

The verb *decompose* is defined by Merriam-Webster's dictionary as "to separate into constituent parts or elements…." The scope of HITRUST CSF Assessments commonly feature many elements (e.g., applications, databases, network infrastructure components, departments, and facilities), which may not always be consistent with all elements of the HITRUST CSF requirement statements. During HITRUST assessments it's often necessary to decompose the scope into its constituent parts and rate them individually.

5. We're struggling with the difference between having no policy and having an undocumented policy. How will an assessor know when an undocumented policy is present in an environment and what steps are needed to identify an undocumented policy?

Both 'no policy' scenarios and 'unwritten policy' scenarios share the common characteristic of not having a written policy that addresses the requirement statement. However, two characteristics differentiate "unwritten policy" scenarios: (i) whether management's expectations of the control are well-understood, and (ii) whether the control is consistently performed (even in the absence of a written policy). Table 15 compares the characteristics of "no policy" and "unwritten policy" side-by-side as they apply to the HITRUST CSF requirement statement which states: *The organization provides a process/mechanism to anonymously report security issues*.

Table 15. Differences in 'No Policy' and 'Unwritten Policy'

No policy	Unwritten policy
No policy exists in writing stating management's intent, direction, or expectations regarding the control, i.e., to anonymously report security issues.	(Same)
Management's expectations regarding performance of the control are **not well-understood** by members of the workforce. Asking different employees yields **different perspectives and/or guesses** as to management's expectations (ranging from, "I don't know," to "We don't do that," to "I think we do X," to "We're supposed to do Y").	Management's expectations regarding the performance of the control is **well-understood** by members of the workforce. Interviews with different employees yield **consistent explanations** of management's expectations.
Most people interviewed by the assessor weren't sure if any mechanism was in place to anonymously report security issues. The remainder of those interviewed were sure that the company didn't have any such a mechanism in place.	Everyone interviewed by the assessor spoke about the online portal made available to anonymously report security issues.
Due to the lack of common understanding of management's expectations, the subject matter/control/CSF requirement **is not consistently met/observed/performed.**	The subject matter/control/CSF requirement **is consistently met/observed/performed.** The control is generally in place throughout the organization, thanks in large part to the common understanding of management's expectations.
It's apparent to the assessor and the entity this control is not in place. As such, testing of the implemented maturity level is not possible.	The assessor inspects the online anonymous tip submission portal in support of rating the implemented maturity level.

Endnotes

[i] See NIST Interagency Report (IR) 7358, Program Review of Information Security Management Assistance (PRISMA), available from https://csrc.nist.gov/publications/detail/nistir/7358/final.
[ii] For more information on CMMI, see https://cmmiinstitute.com/cmmi.
[iii] Quoted from NISTIR 7358, p. 2.
[iv] For more information on the PRISMA maturity levels, see https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance/Security-Maturity-Levels.
[v] For more information on the AICPA, see https://www.aicpa.org/about/missionandhistory.html.
[vi] Quoted from a 2017 whitepaper commissioned by Centrify entitled, Stop the Breach: Reduce the likelihood of an Attack through an IAM Maturity Model: A Forrester Consulting Thought Leadership Paper, p. 1. Available from https://www.centrify.com/media/4594046/stop-the-breach.pdf.
[vii] Adapted from NISTIR 7358.
[viii] Self-assessments are defined here as a type of test that can be performed by organization staff, by contractors, or others engaged by management
[ix] For more information on ISO/IEC 27001:2005, see https://www.iso.org/standard/42103.html.
[x] MyCSF is a best-in-class Software as a Service (SaaS) information risk management platform for assessing and reporting information risk and compliance. For more information, see https://hitrustalliance.net/mycsf/.
[xi] For more information on HITRUST CSF Assessments, see https://hitrustalliance.net/csf-assurance/.
[xii] Weights of 25, 25, 25, 15 and 10 for the maturity levels are current until 12/31/2019. The weights of 15, 20, 40, 10 and 15 indicated in Table 3 and in the text following the table are current after 12/31/2019.
[xiii] Quoted from Educause (2017, Mar), Effective Security Metrics: A guide to Effective Security Metrics, available from https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program/resources/information-security-guide/toolkits/effective-security-metrics.
[xiv] Available from https://doi.org/10.6028/NIST.CSWP.04162018.
[xv] Available from https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.
[xvi] For more information, as well as links to other sector guides for implementation of the NIST Cybersecurity Framework, see https://www.us-cert.gov/ccubedvp/cybersecurity-framework.