Updated Scoring Rubric and Updated PRISMA Model

FAQs

FAQs are specific to this webinar. Visit our General FAQs here.

Q: If you conduct a self-assessment prior to December 31, 2019 using the current weighted scale and then conduct a validated assessment after December 31, 2019, will the validated assessment be assessed against the new weights?

A: Yes, as these are two separate assessment submissions.

Q: My organization has been preparing for their validated assessment for over a year; our understanding of the assessment process and decisions for implementation of controls were based on the old scoring weights. How should we proceed?

A: If your validated assessment object has already been created or will be created prior to December 31, 2019, you can continue to use the old scoring weights and there should be no impact. For objects created on or after December 31, 2019, we do not anticipate a significant impact because the most commonly observed scoring combination (Policy, Procedure, and Implemented all at Fully Compliant with no Measured or Managed) would still result in a score of 75 under the new scoring weights.

Q: If the assessment has already been created in MyCSF but isn't going to be submitted until after December 31, 2019, which scoring methodology will be used?

A: Since it's already created it will use the older/current weights of 25, 25, 25, 15, 10. If it's submitted and accepted after December 31, 2019, it will be QA'd against the new rubric.

Q: We were told that because we tested and scored Measured and Managed that 100% of our assessment will go through HITRUST's QA process and the submission date is early December. What is the likelihood that we will be subject to the new rubric?

A: HITRUST does QA on all requirement statements where Measured or Managed were scored; however, this does not impact the check-in process. If you pass all of the automated quality checks, submit prior to December 15, 2019, and remediate any identified check-in items in a timely manner, your assessment should be accepted prior to December 31, 2019 and be allowed to follow the old scoring rubric.

Q: What happens to assessment objects which are currently built in the portal but have not yet been submitted to HITRUST?

A: Since they're already created, they will use the older/current weights of 25, 25, 25, 15, 10. If they are submitted and accepted after December 31, 2019, they will be QA'd against the new rubric; if submitted and accepted prior to December 31, 2019, they will be QA'd using the current rubric.

Q: Will the new weights promote ad-hoc processes and implementations of controls and less focus on the historically foundational part of a security and privacy program – policies?

A: Given the change in weights, it's certainly possible. However, the organizations that have fully implemented controls (with regards to the Implementation level of maturity in the model) will likely have a written policy for those controls. Full compliance with this level of the maturity model also provides the best assurance that information is being protected appropriately.

Q: What does 'accepting risk' for a control requirement mean?

A: The HITRUST CSF provides a framework-based approach to an organization's risk analysis and subsequent control specification, as is explained in https://hitrustalliance.net/content/uploads/2016/01/Leveraging-a-Control-Based-Framework-to-Simplify-the-Risk-Analysis-Process.pdf. Subsequently, once the organization tailors the CSF controls for their specific needs, the resulting control specification must be fully implemented to reduce information security risk to a generally acceptable level. Any gaps in the implementation therefore introduce additional residual risk that must be treated through mitigation, avoidance, transference, or acceptance. You can find more information on risk treatments in the HITRUST Risk Analysis Guide, available from https://hitrustalliance.net/documents/csf_rmf_related/CSFRiskFactorsGuide.pdf.

Q: Will the weight changes increase the number of CAPs expected?

A: It has the potential to increase the number of CAPs due to gaps in implementation but reduce the number of CAPs due to gaps in policies or procedures. That said, the intent of the change is to ensure that organizations that do become certified do so with a smaller number of CAPs.

Q: How do the changes to the PRISMA weights impact currently certified entities?

A: Changes to the PRISMA weights will not impact previously performed assessments, including currently held certifications.

Q: How do you properly score Measured and Managed for controls with yes/no control requirement statements? Ex: "A CISO is appointed."

A: Here's an example of an operational measure over this requirement: On a quarterly basis, the CIO provides an analysis of whether desired IT staffing levels are met to the CEO. This analysis is formalized via a quarterly reporting procedure that spells out the operational aspects of performing this assessment and communicating the results.

Here's an example of an independent metric (Fully Compliant) over this requirement: On an annual basis, the organization's information security function's staffing levels are formally reviewed by an independent consultant. Such reviews are often performed in conjunction with a larger review of the effectiveness of an organization's security program. The final report from this assessment may clearly outline what was measured (staffing levels), by who (consultant), when (during X weeks or months), what information was used to pull the measure (using an employee roster, an org. chart, and detailed responsibility matrices), the intended audience (the CIO). Either the consultant or the CIO charts the results of this review against past reviews of staffing levels of the security function and evaluates results against targets for each key position (e.g., target: one appointed CISO, two analyst FTE's).

An example of a supporting somewhat compliant managed/risk treatment process: The results of this and similar assessments are reported (1) during a monthly infosec steering committee meeting attended by the CIO and department heads, and (2) formally tracked using an issues register in a GRC platform. Meeting minutes are kept which capture the discussion on whether to address noted issues. No written procedure exists outlining the risk treatment process.

Several of us at HITRUST are fans of the book, "How to Measure Anything" by Douglas W. Hubbard, which goes into detail about what constitutes a measurement, what a metric is, etc.

Q: Will the changes in PRISMA weights effect the raw scores for the 15-level maturity ratings? Ex: Maturity level of 3 occurs when the score is less than 71 but greater than 62?

A: No, they will not. The score-to-level mappings are unchanged.

Q: Is it possible to score less than 100% on either Policy and/or Procedure and still score 100% on Implemented?

A: Yes. For example, you might have an undocumented policy (Somewhat Compliant), an undocumented procedure (Somewhat Compliant), and have fully implemented the requirement across your entire scope (Fully Compliant).

Q: What is the rationale for having organizations self-score for a validated assessment? Many organizations struggle with scoring criteria and the assessor scores are what ultimately count. Would it be possible to eliminate that part of the process?

A: No, the assessed entity is responsible for the initial scoring and the role of the external assessor is to validate scoring. Though an assessor can provide guidance on what should be considered when scoring the intent of the requirement itself, management of the assessed entity would have the most insight into the maturity of controls and be in the best position to score them. Remember, the organization is responsible for implementing the HITRUST CSF into their information protection programs. A HITRUST CSF Assessment is conducted simply to provide assurances about their programs to internal and external stakeholders.

Q: Will HITRUST be providing guidance for senior management on re-certifications where controls have remained consistent as to what effect they should expect to see pertaining to the new weights and scoring rubric?

A: Not at this time but it's certainly something we will consider. Our position is that organizations that have been or wish to be certified should be continuously striving for a minimum compliance of 75/75/75/0/0 across all control requirements by addressing any gaps in their requirements as needed, i.e., they should be making progress on any CAPs they may have in place whether required for certification or not (albeit they may be allowed to accept a reasonable amount of excessive residual risk). If this is the case, organizations will not see any change in their certification status due to the change in weights as the sum total of scores for the first three maturity levels remains the same.

Q: Will there be an updated CCSFP course available for individuals who recently received their CCSFP Certification?

A: The CCSFP course has been updated to reflect the changes. Any individuals who recently received their certifications are invited to listen to the replay of the webcast as well as read the whitepaper and the Risk Analysis Guide. Any CCSFP Certified individuals who would like a copy of the updated slide deck used during training are welcome to email support@hitrustalliance.net and the HITRUST Academy team can email a copy. Please note that an updated slide deck will be available November 6, 2019, which will reflect the new MyCSF user interface.

Q: When will the CCSFP Refresher course be updated to reflect the updates?

A: The CCSFP Refresher course has already updated to reflect these changes.

Q: How do assessors/organizations know when assessments are successfully accepted by the HITRUST Assurance team?

A: As of October 4, 2019, MyCSF sends an automated email when an assessment has either been accepted or rejected by HITRUST.

Q: Do the updated PRISMA weights and new scoring rubric apply to interim assessments?

A: No, all interim assessments will be scored using both the PRISMA weights and scoring rubric which were originally used for the initial validated assessment.

Q: Would a control scored on the old rubric yield a different result with the new scoring rubric? Or is it simply clearer wording with the same ideas?

A: If scored correctly, the result should be the same with respect to the overall maturity rating for a requirement statement. The new scoring rubric provides clarity and granularity as to the intent of the Risk Analysis Guide, which has been in place for several years. However, organizations may see changes in the actual score due to the change in how the maturity levels are weighted. This is intentional, as we discussed during the webinar.

Q: Why do these updates not apply to all assessments submitted to - but not accepted by - the HITRUST Assurance team? I.e., why does the submission need to be accepted by December 31, 2019, not simply submitted?

A: Assessments are not ready for QA until they meet the minimum requirements for acceptance and most assessments are accepted without any issues. Basing the timing of the change upon acceptance allows for a clear end date for usage of the old scoring rubric.

Q: Can I submit an assessment prior to December 31, 2019 based upon the updated scoring rubric? If so, how would I indicate that the new rubric was used?

A: Yes you could, but there is no need to indicate the new rubric was used. Since the new rubric more clearly reflects the existing guidance in the Risk Analysis Guide, this should not result in a material change.

Q: Are metrics and measures still required for Managed maturity, or has Managed completely separated from Measured as a criteria area?

A: The nature of the measurement(s) used to drive the Measured level's scores are divorced from the evaluation of the organization's risk treatment process in the Managed level. While it's important to note that Managed cannot be rated higher than Measured, the type of measurement(s) used—albeit a measure or a metric—no longer act as a direct input into the Managed level's rating.

Q: Is there a plan to update the illustrative procedures to include the specific number of elements within a control requirement statement, since this is a large part of utilizing the new scoring rubric?

A: The elements are provided in the illustrative procedures for the Policy maturity level, and of course assessors can (and should) refer to the HITRUST CSF itself if additional information or context is needed. However, our intent is to develop more extensive assessment procedures that are more consistent with the test plans assessors should be developing for their engagements to help facilitate this process. We expect these updated procedures will be available with the CSF v10 release in late 2020.

Q: Does this mean we are meant to be testing supplemental guidance elements, which are often more detailed than elements listed in the CSF? Are we assessing scores for each element individually to then aggregate the requirement statement score?

A: Yes, assessors should evaluate an organization's compliance with all HITRUST CSF elements outlined in the Policy illustrative procedure. This isn't new. All PRISMA maturity levels (not just Policy) should be scored against all elements listed in the Policy illustrative procedure. For example, a requirement statement's Policy illustrative procedure might explain that the organization's policies should contain element A, element B, and element C. In this case:

- The organization's policies should address all three elements
- The organization should have procedures which address all three elements
- The organization should implement/perform all three elements
- Measurements should measure all three elements
- The organization should apply a risk treatment process against any issues noted for any of the three elements

How well an organization meets all elements is a measure of their "coverage" (the horizontal axis on all of the rubric tables). The rubric tables are built in such a way to easily facilitate the scoring of an environment which meets only some elements and not others.

Q: For the Policy scoring example, Tier 1 said 'Undocumented' but was scored at 100%; is that correct? And why?

A: Possible "tiers" of a policy strength range from tier 0 (no policy) to tier 4 (written, communicated, and approved policy). A policy with a tier 1 strength is one that is undocumented. In the Policy example in the webinar (slide 17), it was the coverage (not the strength) that was rated at 100%. That example was exploring a binary requirement statement (one that had only one element in its Policy illustrative procedure). For binary requirement statements, Policy coverage is either 0% or 100%--the policy either addresses the one element or it does not.

Q: Should Policy be scored according to the illustrative procedures and include all listed points or just on the requirement statement itself?

A: The former. All PRISMA maturity levels (not just Policy) should be scored against all elements listed in the Policy illustrative procedure. For example, a requirement statement's Policy illustrative procedure might explain that the organization's policies should contain element A, element B, and element C. In this case:

- The organization's policies should address all three elements
- The organization should have procedures which address all three elements
- The organization should implement/perform all three elements
- Measurements should measure all three elements
- The organization should apply a risk treatment process against any issues noted for any of the three elements

Q: What type of score would we expect for an undocumented procedure that addresses 100% of the CSF elements?

A: Per the rubric, Somewhat Compliant.

Q: If Implementation has been scored at less than 100%, can Measured still receive a score above 0%?

A: Yes. In this case, the measurement would indicate that a gap exists.

Q: Will this change how scores appear in the MyCSF tool?

A: No, the user interface for scoring will remain the same.

Q: Some v9 baseline statements have become much more complex than v8 baseline statements, sometimes including long lists of requirements. How does one approach scoring complex requirements, and is there an effort to make complex requirements simpler?

A: We touched on this during the webinar but you can find a more detailed explanation with more examples in our associated whitepaper, which may be downloaded from https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

Q: Are HITRUST requirement statements vetted against the new rubric?

A: The guidelines in MyCSF used to assess the requirement statements haven't changed. The new rubric simply incorporates this guidance better than in the original rubric. Subsequently, we do not anticipate any issues with the rubric unless assessors were not following the methodology outlined in the HITRUST Risk Analysis Guide. Regardless, we intend to keep an eye on this and, should any issues arise, 'tweak' the rubric as needed to ensure it is applied appropriately.

Q: Are assessors/assessed entities expected to submit documentation behind the scoring as per the new rubric?

A: Assessors are expected to comply with HITRUST Assurance Bulletin HAA 2019-001's requirements around providing evidence, but (while recommended) assessors are not being required to share the details of any scoring calculations performed when varied scoping elements must be averaged to reach an overall score.

Q: If 25 samples have been tested across 2 different in-scope systems (ex: workstations) and we have a partial-samples failing (ex: 10 failings), how do we consider the sample-based failures in scoring as against score-based?

A: Please refer to the whitepaper. We've got an example there with multiple scoping elements all scoring differently, and we take this example all the way through Managed. The answer: You'd rate each in-scope system individually and then average the scores together to reach an overall rating. For example:

i. If system A had 25 of 25 samples pass, system A would rate Fully Compliant (100%) (assuming very high Implementation coverage), as the 100% pass rate falls within tier 4 Implementation strength.

ii. If system B had 15 of 25 samples pass, system B would rate Partially Compliant (50%) (assuming very high Implementation coverage), as the 60% pass rate falls within tier 2 Implementation strength.

iii. The average of system A's Fully Compliant (100%) and system B's Partially Compliant (50%) is 75%, which is Mostly Complaint.

Q: Where can I find an example which includes multiple elements?

A: Please refer to the whitepaper. We have an example there with multiple scoping elements all scoring differently, and we take this example all the way through Managed.

Q: Where can I find an example which includes a written procedure with multiple elements, including the procedure itself for reference?

A: Please refer to the whitepaper. We have an example there with multiple scoping elements all scoring differently, and we take this example all the way through Managed. However, note that HITRUST does not provide any examples of the procedure language itself.