HITRUST Assurance Advisories

Updated PRISMA weights and scoring rubrics

Oct. 2, 2019
Today’s speakers

Dr. Bryan Cline
Chief Research Officer

Bimal Sheth
VP, Assurance Services

Jeremy Huval
VP, Compliance
Agenda

• Introductions

• HAA 2019-07: Updated PRISMA weights

• HAA 2019-09: Updated scoring rubric

• Your questions
HAA-2019-07

Updated PRISMA level weights
First, some context

5 levels of control maturity

<table>
<thead>
<tr>
<th></th>
<th>Policy</th>
<th>Procedure</th>
<th>Implemented</th>
<th>Measured</th>
<th>Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Compliant</td>
<td>NC</td>
<td>NC</td>
<td>NC</td>
<td>NC</td>
<td>NC</td>
</tr>
<tr>
<td>Somewhat Compliant</td>
<td>SC</td>
<td>SC</td>
<td>SC</td>
<td>SC</td>
<td>SC</td>
</tr>
<tr>
<td>Partially Compliant</td>
<td>PC</td>
<td>PC</td>
<td>PC</td>
<td>PC</td>
<td>PC</td>
</tr>
<tr>
<td>Mostly Compliant</td>
<td>MC</td>
<td>MC</td>
<td>MC</td>
<td>MC</td>
<td>MC</td>
</tr>
<tr>
<td>Fully Compliant</td>
<td>FC</td>
<td>FC</td>
<td>FC</td>
<td>FC</td>
<td>FC</td>
</tr>
</tbody>
</table>

Ratings drive the % of level’s points awarded

0% 25% 50% 75% 100%

"Weights" are the levels’ total possible points

25 pts. 25 pts. 25 pts. 15 pts. 10 pts.
15 pts. 20 pts. 40 pts. 10 pts. 15 pts.

New weights for objects created 12/31/19 and later
Why make this change?

New weights better reflect the value that each PRISMA level and level pair brings to managing information risk:

- **Implemented > any other level**
- **(P+P) > (M+M)**
- **Managed > Measured**
- **Procedure > Policy**
What does this mean in practice?

Let's walk through an example

<table>
<thead>
<tr>
<th>Policy</th>
<th>Procedure</th>
<th>Implemented</th>
<th>Measured</th>
<th>Managed</th>
<th>Score</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully Compliant</td>
<td>Fully Compliant</td>
<td>Fully Compliant</td>
<td>Non-Compliant</td>
<td>Non-Compliant</td>
<td>75 / 100</td>
<td>3+</td>
</tr>
<tr>
<td>Old weights</td>
<td>100% of 25 points</td>
<td>100% of 25 points</td>
<td>+ 0% of 15 pts.</td>
<td>+ 0% of 10 pts.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>New weights</td>
<td>100% of 15 points</td>
<td>+ 100% of 20 pts.</td>
<td>+ 0% of 10 pts.</td>
<td>+ 0% of 15 pts.</td>
<td></td>
<td>3+</td>
</tr>
</tbody>
</table>

Let's walk through an example
What does this mean in practice?

Let’s walk through another example

<table>
<thead>
<tr>
<th>Policy</th>
<th>Procedure</th>
<th>Implemented</th>
<th>Measured</th>
<th>Managed</th>
<th>Score</th>
<th>Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fully Compliant</td>
<td>Fully Compliant</td>
<td>Partially Compliant</td>
<td>Non-Compliant</td>
<td>Non-Compliant</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100% of 25 points</td>
<td>100% of 25 points</td>
<td>50% of 25 points</td>
<td>+ 0% of 15 pts.</td>
<td>+ 0% of 10 pts.</td>
<td>= 62.5 / 100</td>
<td>3</td>
</tr>
<tr>
<td>New weights</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>100% of 15 points</td>
<td>+ 100% of 20 pts.</td>
<td>+ 50% of 40 pts</td>
<td>+ 0% of 10 pts.</td>
<td>+ 0% of 15 pts.</td>
<td>= 55 / 100</td>
<td>3-</td>
</tr>
</tbody>
</table>
HAA-2019-09

Updated scoring rubrics

To download the new rubrics document:
HITRUSTAlliance.net > Downloads > Publicly Available Downloads > CSF Assurance and Related Programs > HITRUST CSF Control Maturity Scoring Rubrics
First, some context

- The rubric is a practice aid used to help determine scores
- Used by assessors and assessed entities during self-assessments and validated assessments
- Usage context:
  - I’m faced with a set of facts about how the organization is (or is not) meeting a HITRUST CSF requirement.
  - Given what I know, how should the Policy level be rated, how should the Implemented level be rated, etc.?
Why change the rubric?

- **Ease of use enhancements** should contribute to more consistent interpretation

- **Fit for Purpose Enhancements:**
  - Originally meant to be a “decision-making tool of last resort,” only to be referred to AFTER having studied the HITRUST Risk Analysis Guide
  - The rubric turned into the sole tool used to scoring determinations - *It was never meant to serve this purpose*
  - This update makes the rubrics document fit for the way it is currently being used
### HITRUST CSF Control Maturity Scoring Rubrics

#### Tier 1
- Documented with all formal policy criteria addressed
- Documented with >1, but not all, formal policy criteria addressed
- Documented with only 1 formal policy criterion addressed
- Undocumented policy
- No policy

#### Tier 2
- Documented with all formal procedural criteria addressed
- Documented with >1, but not all, formal procedural criteria addressed
- Documented with only 1 formal procedural criterion addressed
- Undocumented procedure
- No procedure

#### Tier 3
- No measurements used

#### Tier 4
- Measurement(s) used include an independent measure
- Measurement(s) used include an operational measure

### Measured
- % of CSF policy elements1 addressed by the organization's measurement (Coverage)

### Managed
- % of CSF policy elements1 addressed by the organization's procedure (Coverage)

### Implemented
- % of CSF policy elements1 implemented (Coverage)

#### Procedure
- Frequency of applying risk treatment (Coverage, as a % of issues identified)

#### Policy
- Risk Treatment Process Strength
- Procedural Strength

### Managed rating cannot exceed measured rating

---

**Legend**

<table>
<thead>
<tr>
<th>Rating</th>
<th>Range of Averaged Scores</th>
<th>Points Awarded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Compliant</td>
<td>0% - 10%</td>
<td>0% of points awarded</td>
</tr>
<tr>
<td>Somewhat Compliant</td>
<td>11% - 32%</td>
<td>25% of points awarded</td>
</tr>
<tr>
<td>Partially Compliant</td>
<td>33% - 65%</td>
<td>50% of points awarded</td>
</tr>
<tr>
<td>Mostly Compliant</td>
<td>66% - 89%</td>
<td>75% of points awarded</td>
</tr>
<tr>
<td>Compliant</td>
<td>90% - 100%</td>
<td>100% of points awarded</td>
</tr>
</tbody>
</table>

---

1. As specified in the policy level’s illustrative procedure in MyCSF.
Feeling overwhelmed?

Resources are available to help you apply these new rubrics:

- We’ve recently published a whitepaper on using the new rubrics (including several examples)

- The CCSFP course was recently updated to address this change
When is the go-live date?

• New rubrics must be observed for objects **submitted and accepted on or after 12/31/19**

• In-progress assessments using current rubric must be **accepted** by HITRUST prior to 12/31/19
  
  • “Accepted” = Successful check-in

  • Submission of a validated assessment within MyCSF is the first step towards acceptance

  • After submission, the Assurance team performs certain quality checks; should any of these checks fail, the submission is reverted to the Assessor for remediation
A basic example

**Requirement statement:** “Access to network equipment is physically protected”

**Step 0)** Before diving into testing, first identify and count the CSF policy elements in the policy illustrative procedure.

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). 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 element(s) and determine if the element(s) is/are understood. Evidence of ad hoc or informal policy may also be provided by observing individuals, systems and/or processes associated with responsibilities for the physical protection of network equipment to determine if the policy elements are generally understood and implemented consistently. Review any written procedure(s) or examine documentation associated with formal or ad hoc processes to determine if the requirement(s) is/are addressed consistently by the entity.
## Scoring the POLICY level

**Requirement statement:** “Access to network equipment is physically protected”

### Step 1) Identify relevant policies (even unwritten ones)

### Step 2) Test policies to determine policy coverage

- Since this example only has 1 CSF policy element, we’ll either be at 0% or 100% coverage

### Step 3) Test policy context to determine policy strength against HITRUST's formal policy criteria

### Step 4) Plug in what you’ve learned into the POLICY rubric to reach a rating

### Table: Scoring Policies

<table>
<thead>
<tr>
<th>If the assessor learns that there’s:</th>
<th>This example’s policy strength rated at:</th>
<th>This example’s policy coverage rated at:</th>
<th>This example’s policy level rating:</th>
</tr>
</thead>
<tbody>
<tr>
<td>No policy addressing this</td>
<td>Tier 0</td>
<td>Very low (0%)</td>
<td>NC</td>
</tr>
<tr>
<td>An undocumented policy only</td>
<td>Tier 1</td>
<td>Very high (100%)</td>
<td>SC</td>
</tr>
<tr>
<td>A written policy that spells out expectations but has never been approved or communicated</td>
<td>Tier 2</td>
<td>Very high (100%)</td>
<td>PC</td>
</tr>
<tr>
<td>An approved written policy that spells out expectations but has never been communicated</td>
<td>Tier 3</td>
<td>Very high (100%)</td>
<td>MC</td>
</tr>
<tr>
<td>An approved, communicated written policy that spells out expectations</td>
<td>Tier 4</td>
<td>Very high (100%)</td>
<td>FC</td>
</tr>
</tbody>
</table>
Scoring the PROCEDURE level

Requirement statement: “Access to network equipment is physically protected”

Testing the procedure level is very similar:

Step 1) Identify relevant procedures (even unwritten ones)

Step 2) Determine procedure coverage

Step 3) Determine procedure strength against HITRUST’s formal procedure criteria

Step 4) Plug in what you’ve learned into the PROCEDURE rubric
Scoring the IMPLEMENTED level

**Requirement statement:** “Access to network equipment is physically protected”

**Step 1)** Identify the population of relevant scoping elements

**Step 2)** Test the control’s implementation to determine strength and coverage levels

- Again, since this example only has 1 CSF policy element, we’ll either be at 0% or 100% coverage
- Here the real work will be around determining implementation strength

**Step 3)** Plug what you’ve learned into the rubric to determine a rating

<table>
<thead>
<tr>
<th>Of in-scope networking devices, if the assessor learns that:</th>
<th>This example’s implementation strength:</th>
<th>This example’s implementation coverage:</th>
<th>This example’s implemented rating:</th>
</tr>
</thead>
<tbody>
<tr>
<td>None were physically protected</td>
<td>Tier 0</td>
<td>Very low (0%)</td>
<td>NC</td>
</tr>
<tr>
<td>11% - 32% were physically protected</td>
<td>Tier 1</td>
<td>Very high (100%)</td>
<td>SC</td>
</tr>
<tr>
<td>33% - 65% were physically protected</td>
<td>Tier 2</td>
<td>Very high (100%)</td>
<td>PC</td>
</tr>
<tr>
<td>66% - 89% were physically protected</td>
<td>Tier 3</td>
<td>Very high (100%)</td>
<td>MC</td>
</tr>
<tr>
<td>90% - 100% were physically protected</td>
<td>Tier 4</td>
<td>Very high (100%)</td>
<td>FC</td>
</tr>
</tbody>
</table>
Your Questions
For more information on HITRUST's Programs visit www.HITRUSTAlliance.net

To view our latest documents, visit the Content Spotlight