### HITRUST CSF® Control Maturity Scoring Rubrics

#### POLICY

<table>
<thead>
<tr>
<th>Policy Strength</th>
<th>Tier 0</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
<th>Tier 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No policy</td>
<td>Documented with only 1 formal policy criterion addressed</td>
<td>Documented with only 1 formal procedural criterion addressed</td>
<td>Undocumented procedure</td>
<td>Documented with &gt;1, but not all, formal policy criteria addressed</td>
</tr>
</tbody>
</table>

#### PROCEDURE

<table>
<thead>
<tr>
<th>Procedure Strength</th>
<th>Tier 0</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
<th>Tier 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No procedure</td>
<td>Documented with only 1 formal procedural criterion addressed</td>
<td>Documented with &gt;1, but not all, formal policy criteria addressed</td>
<td>Undocumented procedure</td>
<td>Documented with &gt;1, but not all, procedural criterion addressed</td>
</tr>
</tbody>
</table>

#### IMPLEMENTED

<table>
<thead>
<tr>
<th>Implementation Strength</th>
<th>Tier 0</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
<th>Tier 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No risk treatment process</td>
<td>Documented with only 1 formal procedural criterion addressed</td>
<td>Documented with &gt;1, but not all, formal policy criteria addressed</td>
<td>Undocumented procedure</td>
<td>Documented with &gt;1, but not all, procedural criterion addressed</td>
</tr>
</tbody>
</table>

#### MEASURED

<table>
<thead>
<tr>
<th>Measurement Strength</th>
<th>Tier 0</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
<th>Tier 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No measurements used</td>
<td>Measurement(s) used include an independent metric</td>
<td>Measurement(s) used include an operational metric</td>
<td>Measurement(s) used include an independent measure</td>
<td>Measurement(s) used include an independent metric</td>
</tr>
</tbody>
</table>

#### MANAGED

<table>
<thead>
<tr>
<th>Risk Treatment Process Strength</th>
<th>Tier 0</th>
<th>Tier 1</th>
<th>Tier 2</th>
<th>Tier 3</th>
<th>Tier 4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No risk treatment process</td>
<td>Documented with only 1 formal risk treatment process criterion addressed</td>
<td>Documented with &gt;1, but not all, formal risk treatment process criterion addressed</td>
<td>Undocumented risk treatment process</td>
<td>Documented with all formal risk treatment process criterion addressed</td>
</tr>
</tbody>
</table>

#### 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>Fully Compliant</td>
<td>90% - 100%</td>
<td>100% of points awarded</td>
</tr>
</tbody>
</table>

**Managed rating cannot exceed measured coverage**

**Perfom the following steps**

**Step 1) Decompose / separate scope into individual elements against which the rubric can be applied**

- Example: Two in-scope data centers (DC1, DC2) each use their own procedure for fire extinguisher maintenance

**Step 2) Apply rubric to each individual scope element**

- Example continued: DC1's procedure scores as Mostly Compliant (75%) and DC2’s procedure scores as Non-Compliant (0%)

**Step 3) Calculate an average score**

- Example continued: (75% + 0%) / 2 = 37.5%

**Step 4) Refer to the “Range of Averaged Scores” in the legend (right) to determine a rating**

- Example continued: Because 37.5% falls within the range of 33% - 65%, the computed procedure rating is Partially Compliant

**Viable or incomplete implementation scope on the Policy, Procedure, Measured, or Managed levels?**

v. HT-134-01
**Measurement Concepts**

**MEASUREMENT**
- The process of data collection, analysis, and reporting.
- Examples of measurements in the context of the HITRUST CSF include information obtained from user access reviews, compliance checks, dashboards, alerts, health reports, and audits.

**MEASURE**
- The results of data collection, analysis, and reporting.
- 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).

**METRIC**
- A quantifiable entity that allows the measurement of the performance, (2) be used at an appropriate frequency, and (3) be supported by documentation that addresses specifically:
  - (i) what is measured,
  - (ii) who is responsible for gathering the data,
  - (iii) how the measurement is performed / calculated, and
  - (iv) how often the measurement is reviewed and by whom.

**Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of related performance-related data.**

**To be classified as metric for HITRUST CSF assessment purposes, the measure must meet ALL elements for a metric (listed above) AND:**
- (i) be tracked over time, and
- (ii) have explicitly stated (not implied), established thresholds (i.e., upper and/or lower bounds on a value) or targets (i.e., targeted goals, which the organization is trying to achieve).

**Other Key Concepts**

**OPERATIONAL**
- With respect to a metric or, one that is not influenced by the person or entity that is responsible for the requirement/control being tracked by the measure or metric.

**INDEPENDENT**
- With respect to an assessor or measure, one that is not influenced by the person or group responsible for the requirement or control being measured (e.g., the control owner).

**AUTOMATED CONTROLS**
- Controls that have been programmed, controlled, or embedded within a system.

**PROCEDURE**
- A detailed description of the steps necessary to perform specific operations in conformance with applicable standards.

**FORMAL DOCUMENTED PROCEDURAL CRITERIA:**
- (i) demonstrably approved by management,
- (ii) demonstrably communicated to stakeholders,
- (iii) outlines stakeholder responsibilities,
- (iv) discusses operational aspects such as how, when, and on what the action / control / requirement is to be performed.

**RISK TREATMENT**
- Selecting and implementing mechanisms to modify risk.

**UNDOCUMENTED**
- Not supported by written procedures.

---

**Sample Sizes**

<table>
<thead>
<tr>
<th>Testing a manual control operating at a defined frequency</th>
<th>Minimum Number of Items to Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Daily controls: 25 days</td>
<td>• Pop. size: 20-25 items</td>
</tr>
<tr>
<td>• Weekly controls: 5 weeks</td>
<td>• Pop. size 50-249: 10% of the population, rounding up as needed</td>
</tr>
<tr>
<td>• Monthly controls: 2 months</td>
<td>• Pop. size &lt;50: Sample size can range from a minimum of 3 items up to the entire population.</td>
</tr>
<tr>
<td>• Quarterly controls: 2 quarters</td>
<td>Use professional judgment</td>
</tr>
<tr>
<td>• Annual controls: 1 year</td>
<td>Testing an automated control (NOTE: If configured on or embedded within multiple systems/tools, each system/tool must be tested)</td>
</tr>
</tbody>
</table>

**Timeframes**
- Access window for a HITRUST MyCSF “Report Only” object:
  - 50 calendar days for validated assessment objects, 60 calendar days for interim assessment objects
- Assessor’s validated assessment fieldwork window (maximum):
  - 90 calendar days from the date of submission of the validated assessment object to HITRUST
- Minimum number of days that a remediated or newly implemented control must operate prior to assessor testing:
  - 90 calendar days past the control’s implementation or remediation
- Maximum age of testing performed by the organization (e.g., by Internal Audit) being relied upon by the assessor:
  - 120 days before the 1-year anniversary of the HITRUST CSF Certification (Based on the HITRUST CSF Validated Report’s date)
- Targeted window for HITRUST’s performance of QA and draft report assembly procedures:
  - 56 calendar days (8 weeks), following acceptance / successful check-in of the submission in MyCSF
- Interval assessment object submission due date:
  - No later than the 1-year anniversary of the HITRUST CSF Certification (Based on the HITRUST CSF Validated Report’s date)

---

**Guidance**

**Definition(s)**

**Other Key Concepts**

**With respect to a metric or, one that is not influenced by the person or entity that is responsible for the requirement/control being tracked by the measure or metric.**

*HITRUST Glossary of Terms (v) how often the measure is reviewed and by whom.

*ISACA Glossary of Terms (i) what is measured,

*ENISA Glossary of Terms (ii) demonstrably communicated to stakeholders,

*Cambridge Dictionary (iii) clearly communicates management’s expectations of the control(s) operation (e.g., using “shall”, “will”, or “must” statements).”

---

© 2019 HITRUST All rights reserved. Any commercial uses or derivations of these works are prohibited. No part of this publication may be reproduced or utilized other than being shared as is in full, in any form or by any means, electronic or mechanical, without HITRUST’s prior written permission.