HITRUST CSF® Control Maturity Scoring Rubrics

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

POLICY

	Policy Strength	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
		% of CSF policy elements‡ addressed by the organization's policy (Coverage)				
Tier 4	Documented with all formal policy criteria addressed	NC	SC	PC	MC	FC
Tier 3	Documented with >1, but not all, formal policy criteria addressed					
Tier 2	Documented with only 1 formal policy criterion addressed					
Tier 1	Undocumented policy					
Tier 0	No policy					

PROCEDURE

	Procedure Strength	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
		% of CSF policy elements‡ addressed by the organization's procedure (Coverage)				
Tier 4	Documented with all formal procedural criteria addressed	NC	SC	PC	MC	FC
Tier 3	Documented with >1, but not all, formal criteria attributes addressed					
Tier 2	Documented with only 1 formal procedural criterion addressed					
Tier 1	Undocumented procedure					
Tier 0	No procedure					

IMPLEMENTED

	Implementation Strength (As a % of scope elements, e.g., systems, facilities)	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
		% of CSF policy elements‡ implemented (Coverage)				
Tier 4	90% - 100% of scope	NC	SC	PC	MC	FC
Tier 3	66% - 89% of scope					
Tier 2	33% - 65% of scope					
Tier 1	11% - 32% of scope					
Tier 0	0% - 10% of scope					

MEASURED

	Measurement Strength	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
		% of CSF policy elements‡ addressed by the organization's measurement (Coverage)				
Tier 4	Measurement(s) used include an independent metric	NC	SC	PC	MC	FC
Tier 3	Measurement(s) used include an operational metric					
Tier 2	Measurement(s) used include an independent measure					
Tier 1	Measurement(s) used include an operational measure					
Tier 0	No measurements used					

MANAGED

	Risk Treatment Process Strength	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
		Frequency of applying risk treatment (Coverage, as a % of issues identified for the CSF Policy elements‡)				
Tier 4	Documented with all formal risk treatment process criteria addressed	NC	SC	PC	MC	FC
Tier 3	Documented with >1, but not all, formal risk treatment process criteria addressed					
Tier 2	Documented with only 1 formal risk treatment process criterion addressed					
Tier 1	Undocumented risk treatment process					
Tier 0	No risk treatment process OR measured score = NC					

Managed rating cannot exceed measured coverage

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

Perform 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

Legend

Rating	Range of Averaged Scores	Points Awarded
Non-Compliant	0% - 10%	0% of points awarded
Somewhat Compliant	11% - 32%	25% of points awarded
Partially Compliant	33% - 65%	50% of points awarded
Mostly Compliant	66% - 89%	75% of points awarded
Fully Compliant	90% - 100%	100% of points awarded

Timeframes

Window	Duration
Access window for a HITRUST MyCSF "Report Only" object	90 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	90 calendar days, as determined by comparing the external assessor's fieldwork start date of the internal assessor's fieldwork start date
Maximum age of third-party assessments/inspections/audits being relied upon by the assessor	1 year, as determined by comparing the HITRUST CSF validated assessment fieldwork start date to: • Period end date (for period-of-time reports) • Final report date (for point-in-time reports or forward-looking certifications)
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
Window during which HITRUST will accept grammatical changes to a draft report	30 calendar days from issuance of draft report
Days allowed for Corrective Action Plans (CAPs) to be entered into MyCSF	30 calendar days from issuance of draft report
Validity window for a HITRUST CSF Certification	2 years from the HITRUST CSF Validated Report's date. Requires successful completion of an interim assessment to remain valid for the 2-year period.
Earliest that an interim assessment can begin (i.e., earliest that an interim assessment object can be created in MyCSF)	120 days before the 1-year anniversary of the HITRUST CSF Certification (based on the HITRUST CSF Validated Report's date)
Interim 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)

Sample Sizes

Sampling Scenario	Minimum Number of Items to Test
Testing a manual control operating at a defined frequency	• Daily controls: 25 days • Weekly controls: 5 weeks • Monthly controls: 2 months • Quarterly controls: 2 quarters • Annual controls: 1 year (most recent control occurrence)
Testing a manual control operating at an undefined frequency (i.e., "as needed")	**Sample size varies based on population size:** • Pop. size >=250: 25 items • Pop. size 50-249: 10% of the population, rounding up as needed • Pop. size <50: Sample size can range from a minimum of 3 items up to the entire population. Use professional judgment.
Testing an automated control (NOTE: If configured on or embedded within multiple systems/tools, each system/tool must be tested)	**Can perform a test of 1 if the following are performed / met** (otherwise, a full sample must be tested using the manual control sampling guidance provided above): • If configurable, the associated configuration(s) must be tested • To show that system behaves as configured, the outcome / result of the configuration must be tested
Sampling from point-in-time populations (e.g., endpoints, servers)	Observe the sampling guidance provided for the "Testing a manual control with an undefined frequency" scenario provided above

Measurement Concepts

Definition(s)	Guidance
MEASUREMENT	
The process of data collection, analysis, and reporting. *[NIST CSRC Glossary of Terms]* 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]*	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. *[NIST CSRC Glossary of Terms]* 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 of Terms]*	A measure is 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: (i) what is measured, (ii) who is responsible for gathering the data, (iii) how the data is recorded, (iv) how the measurement is performed / calculated, and (v) how often the measure is reviewed and by whom.
METRIC	
Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data. *[NIST CSRC Glossary of Terms]* 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 of Terms]* 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. *[Educause (2017, Mar). Effective Security Metrics: A guide to Effective Security Metrics]*	**To be classified as metric for HITRUST CSF assessment purposes**, the measurement must meet ALL requirements for a measure (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, what the organization is trying to achieve).

Please consult the following white paper for additional guidance:
https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf

Other Key Concepts

Definition(s)	Guidance
OPERATIONAL	
With respect to a measure or metric, one that is produced by, or otherwise influenced by, the person or entity responsible for the requirement/control being tracked by the measure or metric. *[HITRUST Glossary of Terms]*	**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.).
INDEPENDENT	
With respect to an assessor or measure, one that is not influenced by the person or entity that is responsible for the requirement/control being evaluated or measured. *[HITRUST Glossary of Terms]*	**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).
AUTOMATED CONTROLS	
Controls that have been programmed, configured, and/or embedded within a system. *[ISACA Glossary of Terms, adapted]*	**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.
PROCEDURE	
A detailed description of the steps necessary to perform specific operations in conformance with applicable standards. Procedures are defined as part of processes. *[ISACA Glossary of Terms, adapted]*	**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, who, and on what the action / control / requirement is to be performed.
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. *[ISACA Glossary of Terms, adapted]*	**Formal documented policy criteria:** (i) demonstrably approved by management, (ii) demonstrably communicated to stakeholders in the organization and members of the workforce, and (iii) clearly communicates management's expectations of the control(s) operation (e.g., using "shall", "will", or "must" statements).
RISK TREATMENT	
Selecting and implementing mechanisms to modify risk. Risk treatment options can include avoiding, optimizing, transferring, or retaining [accepting] risk. *[ENISA Glossary of Terms]*	**Formal documented risk treatment process criteria:** (i) 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, (ii) a defined mechanism to track issues, risks, and risk treatment decisions, and (iii) cost, level of risk, and mission impact are considered in risk treatment decisions.
UNDOCUMENTED	
Not supported by written proof. *[Cambridge Dictionary]*	**Undocumented policies, procedures, and processes are those that are:** (i) well-understood by those required to implement them and / or adhere to them, (ii) consistently observed, and (iii) unwritten.