HITRUST Control Maturity Scoring Rubric (version 4)

POLICY†

	Policy Strength	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
Tier 2	Documented policy	NC	SC	PC	MC	FC
Tier 1	Undocumented policy					
Tier 0	No policy					

% of evaluative elements‡ addressed by the organization's policy (Coverage)

PROCEDURE†

	Procedure Strength	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
Tier 2	Documented procedure	NC	SC	PC	MC	FC
Tier 1	Undocumented procedure					
Tier 0	No procedure					

% of evaluative elements‡ addressed by the organization's procedure (Coverage)

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%
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					

% of evaluative elements‡ implemented (Coverage)

Used for e1, i1, and r2 assessments

MEASURED

	Measurement Strength	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
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					

% of evaluative elements‡ addressed by the organization's measurement (Coverage)

MANAGED

	Risk Treatment Process Strength	Very Low 0% - 10%	Low 11% - 32%	Moderate 33% - 65%	High 66% - 89%	Very High 90% - 100%
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					

Frequency of applying risk treatment (Coverage, as a % of issues identified for the evaluative elements‡)

Managed rating cannot exceed measured coverage

For varied or incomplete scope on each level, 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 the HITRUST CSF control maturity scoring 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	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

† HITRUST does not require that policy statements reside in only policy documents or that procedures reside in only procedure documents. They can reside in documents identified as standards, handbooks, guidelines, directives, etc.

‡ For CSF v9.x: As specified in the policy illustrative procedures (r2 assessments) and/or evaluative elements (i1 assessments). For CSF v11: As specified in the requirement statements (e1, i1, and r2 assessments).

Timeframes

Window	Duration
Assessor's validated assessment fieldwork window (maximum)	*r2, i1, and e1:* 90 calendar days from the start of the fieldwork period for the HITRUST validated assessment.
Minimum number of days that a remediated or newly implemented control must operate prior to assessor testing (i.e., incubation period)	• 60 calendar days for a new or remediated policy or procedure • 90 calendar days for a new or remediated control at the implementation, measured and/or managed maturity levels
Maximum age of testing performed by the organization (e.g., by an Internal Assessor) being relied upon by the external assessor	90 calendar days, as determined by comparing the external assessor's fieldwork start date to the internal assessor's fieldwork start date
Maximum age of third-party assessments/inspections/audits being relied upon by the assessor	One year, as determined by comparing the HITRUST 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)
Validity window for a HITRUST Certification	*r2:* Two years from HITRUST Certification date. Requires completion of interim assessment at one-year anniversary. *i1 and e1:* One year from HITRUST certification date.
Earliest that an interim assessment can begin (or interim assessment object can be created in MyCSF)	120 days before the one-year anniversary of the HITRUST Certification (based on the HITRUST Validated Report's date)
Bridge certificate timing considerations *Note: Bridge certificates are only available for r2 validated assessments with certification. Additional guidance on bridge certificates can be found at* HITRUST-CSF-Bridge-Assessment-1.pdf (hitrustalliance.net)	• Bridge certificate is valid for 90 days after the expiration of the previous validated assessment. • Object can be created in MyCSF up to 60 days prior to expiration of the previous certification's expiration. • Bridge must be submitted no more than 30 days before and up to 30 days after the expiration date of previous certification.

Sample-based Testing Requirements

Sampling Scenario	Minimum Number of Items to Test*
Testing a manual control operating at a defined frequency	**The expected frequency of the control must first be defined and then apply the following minimum requirements:** • Daily controls: 25 days • Weekly controls: 5 weeks • Monthly controls: 2 months • Quarterly controls: 2 quarters • Semi-annual controls: 2 halves • 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 is a minimum of 3 items **Population period:** • Minimum of 90 days prior to the date of testing with a maximum of one-year prior to the date of testing
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, current employee list)	Observe the sampling guidance provided for the "Testing a manual control with an undefined frequency" scenario provided above

**Testing lead sheets must be used to document the sampling approach, the items selected for testing, and results of testing for each sampled item. Evidence must be retained to support the conclusions for each sampled item.*

Measurement Concepts

Definition(s)	Guidance
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 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. Examples of measurements in the context of the HITRUST Assurance program include information obtained from user access reviews, compliance checks, dashboards, alerts, health reports, and audits. **To be classified as a measure for HITRUST assessment purposes**, supporting documentation must: (i) address the control's operation / performance, (ii) specify an appropriate frequency, (iii) define what is measured, (iv) identify who is responsible for gathering the data, (v) describe how the data is recorded, (vi) describe how the measurement is performed / calculated, and (vii) specify 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 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).
OPERATIONAL & INDEPENDENT	
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** 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).

Other Key Concepts

Definition(s)	Guidance
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.
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]*	A **documented policy** must specify the mandatory nature of the requirement statement in a written format which could reside in a document identified as a policy, standard, directive, handbook, etc.
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]*	A **documented procedure** must address the operational aspects of how to perform the requirement statement. The procedure should be at a sufficient level of detail to enable a knowledgeable and qualified individual to perform the requirement.
UNDOCUMENTED	
Not supported by written proof. *[Cambridge Dictionary]*	**Undocumented policies and procedures are those that are:** (i) well-understood by those required to implement them and / or adhere to them, (ii) consistently observed, and (iii) unwritten.
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]*	**To be classified as a risk treatment process for HITRUST assessment purposes**, the process must include: (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.

Please consult our HITRUST Assurance Program page and Advisories for additional guidance:
HITRUST Assurance Program - HITRUST Alliance
Advisories - HITRUST Alliance