The below examples outline how the changes to the strength criteria may impact scoring for various scenarios. For reference, please see HITRUST-CSF-Control-Maturity-Scoring-Rubrics.pdf.

Example 1 – Policy Level with a Single Element – Strength Evaluation Difference.

0503.09m1Organizational.6 - Wireless access points are placed in secure locations.

Policy IP - Examine policies and/or standards related to the management of wireless access points and determine if wireless access points are placed in secure areas. Validate the existence of a written policy or standard. Review any written procedures or examine documentation associated with formal or informal processes to determine if the policy/control requirements are addressed consistently by the organization. If a written policy or standard does not exist, interview responsible parties to confirm their understanding of the policy/control requirements. Evidence of an informal policy may be demonstrated by observing individuals, systems, and/or processes associated with said policy or standard to determine if the policy/control requirements are generally understood and implemented consistently.

Assessed Entity Policy Assumptions –

1. Written Policy document
2. Policy document has been approved by management
3. Evidence of communication of the Policy document could not be obtained

Assessed Entity Policy Statement -

"ABC Corporation must place all wireless access points in secure locations."

Scoring –

Strength Criteria	Strength	Coverage	Score	Scoring Discussion
Current Strength Criteria	Tier 3	Very High	Mostly Compliant	The lack of evidence of communication of the policy would mean Policy criteria (ii) was not met. With two of the three criteria met, this would result in a Mostly Compliant score based upon Very High coverage.
Revised Strength Criteria	Tier 4	Very High	Fully Compliant	The written policy document indicates the 'mandatory nature of the control requirement'. The lack of evidence of communication of the policy should not be considered in evaluation of 0503.09m1Organizational.6, but should be considered in evaluation of other requirements within the assessment that address communication of policies.

Example 2 – Policy Level with Multiple Elements - Very Low Coverage

0501.09m1Organizational.1 - Vendor defaults for wireless access points are changed prior to authorizing the implementation of the access point.

Policy IP - Examine policies and/or standards related to the management of wireless access points and determine if when configuring wireless access points and devices the organization changes the following: (i) vendor default encryption keys; (ii) encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions; (iii) default SNMP community strings on wireless devices; (iv) default passwords/passphrases on access points; and (v) other security-related wireless vendor defaults, if applicable. Validate the existence of a written policy or standard. Review any written procedures, or examine documentation associated with formal or informal processes, to determine if the policy/control requirements are addressed consistently by the organization. If a written policy or standard does not exist, interview responsible parties to confirm their understanding of the policy/control requirements. Evidence of an informal policy may be demonstrated by observing individuals, systems, and/or processes associated with said policy or standard to determine if the policy/control requirements are generally understood and implemented consistently.

Assessed Entity Policy Assumptions –

1. Written Policy document
2. Policy document has been approved by management
3. Policy document has been communicated to stakeholders

Assessed Entity Policy Statement –

"ABC Corporation must change vendor default settings for wireless access points prior to implementation of the access point."

Scoring –

Strength Criteria	Strength	Coverage	Score	Scoring Discussion
Current Strength Criteria	Tier 4	Very Low	Non-compliant	The written policy meets all three of the policy criteria; however, it does not address any of the HITRUST CSF policy elements enumerated in the policy illustrative procedure.
Revised Strength Criteria	Tier 4	Very Low	Non-compliant	The written policy document indicates the 'mandatory nature of the control requirement'. The evaluation of coverage does not change.

Example 3 – Policy Level with Multiple Elements – Strength Evaluation Difference

0501.09m1Organizational.1 - Vendor defaults for wireless access points are changed prior to authorizing the implementation of the access point.

Policy IP - Examine policies and/or standards related to the management of wireless access points and determine if when configuring wireless access points and devices the organization changes the following: (i) vendor default encryption keys; (ii) encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions; (iii) default SNMP community strings on wireless devices; (iv) default passwords/passphrases on access points; and (v) other security-related wireless vendor defaults, if applicable. Validate the existence of a written policy or standard. Review any written procedures, or examine documentation associated with formal or informal processes, to determine if the policy/control requirements are addressed consistently by the organization. If a written policy or standard does not exist, interview responsible parties to confirm their understanding of the policy/control requirements. Evidence of an informal policy may be demonstrated by observing individuals, systems, and/or processes associated with said policy or standard to determine if the policy/control requirements are generally understood and implemented consistently.

Assessed Entity Policy Assumptions –

1. Written Policy document
2. Policy document has been approved by management
3. Policy document has been communicated to stakeholders

Assessed Entity Policy Statement –

Wireless Access Points

The organization changes the following: (i) vendor default encryption keys; (ii) encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions; (iii) default SNMP community strings on wireless devices; (iv) default passwords/passphrases on access points; and (v) other security-related wireless vendor defaults, if applicable.

Scoring –

Strength Criteria	Strength	Coverage	Score	Scoring Discussion
Current Strength Criteria	Tier 1	Very High	Somewhat Compliant	The policy document does not meet policy criteria (iii) clearly communicates management's expectations of the control(s) operation (e.g., using "shall", "will", or "must" statements). As a result, the document could not be considered a policy because it could not meet the definition of a policy contained in the rubric, since a list of actions would not be an expression of management's expectations and directions.
Revised Strength Criteria	Tier 4	Very High	Fully Compliant	The written policy document indicates the 'mandatory nature of the control requirement'. The inclusion of the policy illustrative procedure language in a policy document by management meets the revised policy strength criteria.

Example 4 – Procedure Level with a Single Element – Strength Evaluation Difference

0503.09m1Organizational.6 - Wireless access points are placed in secure locations.

Policy IP - Examine policies and/or standards related to the management of wireless access points and determine if wireless access points are placed in secure areas. Validate the existence of a written policy or standard. Review any written procedures, or examine documentation associated with formal or informal processes, to determine if the policy/control requirements are addressed consistently by the organization. If a written policy or standard does not exist, interview responsible parties to confirm their understanding of the policy/control requirements. Evidence of an informal policy may be demonstrated by observing individuals, systems, and/or processes associated with said policy or standard to determine if the policy/control requirements are generally understood and implemented consistently.

Assessed Entity Procedure Assumptions –

1. Written Policy document
2. Procedure document has been approved by management
3. Evidence of communication of the Policy document could not be obtained

Assessed Entity Procedure -

WAP Placement:

- The IT department is the only organization that can install WAPs
- Only install WAPs in rooms that have limited access through the use of badges (e.g.: do not install WAPs in common areas such as the building lobby)
- All WAPs are to be installed in the ceiling
- If ceiling installation is not feasible, WAPs can be installed in a communications closet that is limited to IT department personnel only

Scoring –

Strength Criteria	Strength	Coverage	Score	Scoring Discussion
Current Strength Criteria	Tier 3	Very High	Mostly Compliant	The lack of evidence of communication of the procedure would mean Procedure criteria (ii) was not met. With three of the four criteria met this would result in a Mostly Compliant score based upon Very High coverage.
Revised Strength Criteria	Tier 4	Very High	Fully Compliant	The written procedure document indicates the 'operational aspects of how to perform the requirement'. Additionally, the procedure is written at a sufficient level of detail such that a knowledgeable and qualified individual in the IT department could perform the requirement. The lack of evidence of communication of the procedure should not be considered in evaluation of 0503.09m1Organizational.6, but should be considered in evaluation of other requirements within the assessment that address communication of procedures.

Example 5 – Procedure Level with Multiple Elements - Very Low Coverage

0501.09m1Organizational.1 - Vendor defaults for wireless access points are changed prior to authorizing the implementation of the access point.

Policy IP - Examine policies and/or standards related to the management of wireless access points and determine if when configuring wireless access points and devices the organization changes the following: (i) vendor default encryption keys; (ii) encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions; (iii) default SNMP community strings on wireless devices; (iv) default passwords/passphrases on access points;

and (v) other security-related wireless vendor defaults, if applicable. Validate the existence of a written policy or standard. Review any written procedures, or examine documentation associated with formal or informal processes, to determine if the policy/control requirements are addressed consistently by the organization. If a written policy or standard does not exist, interview responsible parties to confirm their understanding of the policy/control requirements. Evidence of an informal policy may be demonstrated by observing individuals, systems, and/or processes associated with said policy or standard to determine if the policy/control requirements are generally understood and implemented consistently.

Assessed Entity Procedure Assumptions –

1. Written Policy document
2. Policy document has been approved by management
3. Policy document has been communicated to stakeholders

Assessed Entity Procedure –

When the IT department is configuring a WAP, use the ABC Corporation random password generation tool to generate a new password and change the default administrator password on the WAP to one that was newly generated.

Scoring –

Strength Criteria	Strength	Coverage	Score	Scoring Discussion
Current Strength Criteria	Tier 4	Low	Somewhat Compliant	The written procedure meets all four of the procedure criteria; however, it only addresses (iv) of the CSF policy elements enumerated in the policy illustrative procedure.
Revised Strength Criteria	Tier 4	Low	Somewhat Compliant	The written procedure document indicates the 'operational aspects of how to perform the requirement'. Additionally, the procedure is written at a sufficient level of detail such that a knowledgeable and qualified individual in the IT department could perform the requirement. The evaluation of coverage does not change.