HITRUST®

HITRUST CSF v11 FAQs

Why were the evaluative elements moved from the illustrative procedure to the requirement statement?

Per the HITRUST Control Maturity Scoring Rubric, scoring a requirement statement requires locating and parsing the requirement's evaluative elements. To make this task easier, HITRUST has moved the evaluative elements from the policy illustrative procedure to the requirement statement where they are individually numbered. This improves visibility of the evaluative elements without increasing the level of effort to evaluate each requirement statement.

Did any evaluative elements change when they were moved from the illustrative procedures to the requirement statement?

For the vast majority of requirement statements, the evaluative elements did not change – they were simply moved from the illustrative procedures to the requirement statement. In less than 30 requirement statements, when the evaluative elements were relocated to the requirement statement, some evaluative elements were removed, added, or edited for clarity. The CSF Summary of Changes document contains the detailed changes.

What changes have been made to the illustrative procedures?

For all requirement statements in the v11 library, the illustrative procedures have been updated as follows:

- **Policy:** Since the evaluative elements have been moved from the policy level illustrative procedures to the requirement statements, all policy level illustrative procedures have been updated to the following standard text:

  Examine policies related to each evaluative element within the requirement statement. Validate the existence of a written or undocumented policy as defined in the HITRUST Scoring Rubric.
- **Process:** All process level illustrative procedures have been updated to the following standard text:

  Examine evidence that written or undocumented procedures exist as defined in the HITRUST Scoring Rubric. Determine if the procedures address the operational aspects of how to perform each evaluative element within the requirement statement.
- **Implemented:** To enhance usability, the implemented level illustrative procedures have been reformatted:

  Examine evidence that all evaluative elements within the requirement statement have been implemented as defined in the HITRUST Scoring Rubric using a sample based test where indicated below in the example test. If a sample based test is not possible, provide justification to support an alternative testing approach.

  Example test(s):

  <Requirement specific implementation guidance>
- **Measured:** To enhance usability, the measured level illustrative procedures have been reformatted:

  Examine measurements that formally evaluate and communicate the operation and/or performance of each evaluative element within the requirement statement. Determine the percentage of evaluative elements addressed by the organization's operational and/or independent measure(s) or metric(s) as defined in the HITRUST Scoring Rubric. Determine if the measurements include independent and/or operational measure(s) or metric(s) as defined in the HITRUST Scoring Rubric.

  Example test(s):

  <Requirement specific measurement guidance>
- **Managed:** All managed level illustrative procedures have been updated to the following standard text:

  Examine evidence that a written or undocumented risk treatment process exists, as defined in the HITRUST Scoring Rubric. Determine the frequency that the risk treatment process was applied to issues identified for each evaluative element within the requirement statement.

Will the evaluative elements be numbered within the requirement statement in v9.1 – 9.6?

For v9.1 – 9.6, the evaluative elements have been numbered although they remain within the policy level illustrative procedure and have not been moved to the requirement statement.

How does inheritance work between v9.x and v11?

In general v11 assessments can inherit from v9.x assessments and vice versa. However, due to the change to the r2 assessment baseline, if an organization uses v9.x and their service provider uses v11, there may be requirement statements included in the v9.x assessment that are not present in the service provider's v11 assessment and therefore would not be inheritable. To account for this, HITRUST has created a Community Supplemental Requirement factor that inheritance providers are encouraged to select to include additional inheritable 9.x requirement statements into v11 r2 Assessments.

Do the changes to the r2 assessment baseline affect the tailoring of an r2 assessment?

No. For v11, while the r2 assessment baseline has been update, the process of tailoring of the assessment according to the factor responses has not changed.

How many requirement statements will be added or removed from my assessment if I upgrade to v11?

MyCSF subscribers can utilize the preview functionality described in HAA 2021-006 to determine impact on an existing assessment prior to upgrading to v11 including a detailed look at the direct changes that will apply to the assessment.

How different is the v11 r2 core from the v9.x r2 baseline?

The following 58 requirement statements are common between the v11 r2 core and v9.x r2 baseline:

0101.00a1Organizational.123
0104.02a1Organizational.12
0109.02d1Organizational.4
0114.04b1Organizational.1
0117.05a1Organizational.1
0135.02f1Organizational.56
0201.09j1Organizational.124
0226.09k1Organizational.2
0305.09q1Organizational.12
0403.01x1System.8
0415.01y1Organizational.10
0429.01x1System.14
0505.09m2Organizational.3
0601.06g1Organizational.124
0613.06h1Organizational.12
0627.10h1System.45
0709.10m1Organizational.1
0805.01m1Organizational.12
0814.01n1Organizational.12
0816.01w1System.1
0835.09n1Organizational.1
0903.10f1Organizational.1
0913.09s1Organizational.5
0945.09y1Organizational.3
1003.01d1System.3
1107.01b1System.2
1114.01h1Organizational.123
11190.01t1Organizational.3
1129.01v1System.12
1143.01c1System.123
1203.09aa1System.2
12101.09ab1Organizational.3
1239.09aa1System.4
1270.09ad1System.12
1306.06e1Organizational.5
1307.07c1Organizational.124
1408.09e1System.1
1411.09f1System.1
1506.11a1Organizational.21560.11d1 Organizational.1
1589.11c1Organizational.5
1602.12c1Organizational.4567
1616.09l1Organizational.16
1617.09l1Organizational.23
1618.09l1Organizational.45
1634.12b1Organizational.1
1666.12d1Organizational.1235
1704.03b1Organizational.12
17126.03c1System.6
1781.10a1Organizational.23
1802.08b1Organizational.3
18108.08j1Organizational.1
18127.08l1Organizational.3
1826.09p1Organizational.1
1845.08b1Organizational.7
1863.08d1Organizational.4
1903.06d1Organizational.3456711
19142.06c1Organizational.8

The following 124 requirement statements are included in the v11 r2 core and are not included in the v9.x r2 baseline:

01109.02b1Organizational.7
0113.04a1Organizational.2
0126.05b1Organizational.1
0151.02c1Organizational.23
0173.05c1Organizational.45
0180.05h1Organizational.4
0181.06a1Organizational.12
0183.07b1Organizational.1
0193.09a1System.3
0207.09j1Organizational.6
0210.01g1Organizational.1
0217.09j1Organizational.7
0265.09m1Organizational.2
02962.09j1Organizational.5
0302.09o1Organizational.3
0304.09o1Organizational.2
0311.09o1Organizational.5
0321.09u1Organizational.2
0330.09o1Organizational.4
04.01x1Organizational.5
0404.01x1Organizational.5
0407.01y1Organizational.4
0501.09m1Organizational.10
0501.09m1Organizational.11
0502.09m1Organizational.5
0503.09m1Organizational.6
0504.09m1Organizational.13
0506.09m1Organizational.12
06.09b1System.2
0633.10j1System.1
0636.10k1Organizational.3
0666.10h1System.5
0667.10h1System.6
06900.09d1System.2
07.07a1Organizational.8
07.10m1Organizational.2
07.10m1Organizational.3
0701.07a1Organizational.7
0701.07a1Organizational.8
0704.07a1Organizational.8
0704.07a1Organizational.9
0706.10b1System.2
0715.10m1Organizational.4
0732.09r1Organizational.3
0778.10m1Organizational.5
08.09m1Organizational.8
0802.01i1Organizational.2
0815.01o1Organizational.1
0820.01k1System.3
0825.09m1Organizational.14
09.09v1Organizational.7
0905.10g1Organizational.12
0931.09v1Organizational.8
0936.09w1Organizational.1
0939.09x1Organizational.2
0954.10d1System.1
10.01d1System.10
1011.01f1Organizational.1
1013.01r1System.2
1023.01d1System.11
10902.01d1System.12
11.01e1System.2
11.01p1System.5
11.01q1System.3
11.01q1System.4
1101.01a1Organizational.1245
1105.09c1Organizational.2
11124.01s1System.2
11131.01u1System.2
11143.02i1Organizational.3
11149.02g1Organizational.2
11152.02h1Organizational.1
1117.01j1Organizational.23
11183.01c1System.3
1123.01q1System.2
1151.01c1System.2
1194.01l1Organizational.2
12148.06i1Organizational.1
1223.09ac1System.1
1235.06j1Organizational.1
1272.09ae1System.13
1295.09af1System.2
13.02e1Organizational.6
1304.02e1Organizational.7
1308.09j1Organizational.5
13998.02e1Organizational.2
1403.05i1Organizational.67
1414.09g1System.1
1416.10l1Organizational.1
1419.05j1Organizational.12
1428.05k1Organizational.2
1444.09t1Organizational.12
1535.11b1Organizational.12
1561.11c1Organizational.4
1563.11d1Organizational.2
1569.11e1Organizational.12
16.09l1Organizational.4
1611.09h1System.2
1632.12a1Organizational.1
1677.12e1Organizational.6
1701.03a1Organizational.12345678
1734.03d1Organizational.2
1739.05d1Organizational.3
1744.05f1Organizational.23
1749.05g1Organizational.1
1767.07d1Organizational.2
1769.09i1System.12
18122.08k1Organizational.1
18128.08m1Organizational.12
1828.08a1Organizational.12
1857.08c1Organizational.1
1867.08e1Organizational.12
1871.08f1Organizational.13
1880.08g1Organizational.6
1888.08h1Organizational.456
1899.08i1Organizational.1
1908.10c1System.5
19131.05e1Organizational.45
19165.07e1Organizational.13
19180.09z1Organizational.2
19199.10e1System.12
19204.10i1System.1
19249.06b1Organizational.2
19922.06f1Organizational.2

What does a requirement statement and its policy level illustrative procedure look like in v11 compared to v9.x?

See an example below of a requirement statement (BUID 1804.08b2Organizational.12) and the corresponding policy level illustrative procedure in v9.6.2 and v11.

v9.6.2

9. BUID: 1804.08B2ORGANIZATIONAL.12 | CVID: 0703.0

A visitor log containing appropriate information is reviewed monthly and maintained for at least two years.

Evaluative Elements: 10

Illustrative Procedure for Policy	Examine policies and/or standards related to physical security to determine if a visitor log includes the **1)** date **2)** and time of **3)** entry **4)** and departure, **5)** the visitor's name, **6)** the organization represented, **7)** and the employee authorizing physical access. **8)** The log is reviewed no less than monthly **9)** and upon occurrence of organization-defined security events, **10)** and retained for at least two years in accordance with the organization's retention policy. 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.

v11

Illustrative Procedure for Policy	Examine policies related to each evaluative element within the requirement statement. Validate the existence of a written or undocumented policy as defined in the HITRUST scoring rubric.

7. BUID: 1804.08B2ORGANIZATIONAL.12 | CVID: 0703.0

A visitor log includes:
1. the date of entry;
2. time of entry;
3. date of departure;
4. time of departure;
5. the visitor's name;
6. the organization represented; and
7. the employee authorizing physical access.

The log is reviewed
8. no less than monthly and
9. upon occurrence of organization-defined security events.

The log
10. is retained for at least two years in accordance with the organization's retention policy.

What does it mean for an Authoritative Source to be refreshed?

An authoritative source refresh is an update to a previously mapped authoritative source due to a change in the authoritative source or in order to refine the mapping using the NIST OLIR methodology.

Now that the r2 is threat adaptive how do I do readiness against a moving target?

When the HITRUST quarterly reconciliation of cyber threat intelligence to the HITRUST CSF requirements results in the need to update the core requirement selection, a new major or minor CSF version will be released. The previous CSF version will remain active for a period of time to provide time to transition to the new version. Based upon the quarterly reconciliations performed in 2022, HITRUST does not expect significant changes in the core requirement selection from one version to the next.

Will the interim and bridge assessments for the r2 be threat adaptive?

No, interim and bridge assessments will continue to use the same CSF version as their corresponding r2 assessments.

What happened to the 75 controls references required for certification?

For the v11 r2 baseline, the level 1 requirements from the 75 controls required by certification have been replaced with the core requirement selection. The core requirement selection is made up of the i1 requirement statements.

How do comprehensive assessments work on an r2 work?

For r2 assessments using v11, the assessment option “Would you like only the controls required for certification or ALL CSF security controls?” has been updated to “Will this be a comprehensive assessment?”. When answered yes, the tailoring of the r2 assessment based on factor responses will include requirement statements across all 135 security control references rather than only the 75 control references required for certification.

Does this change how privacy controls are included in an r2 assessment?

No, privacy controls may still be included using the assessment option “Include privacy controls?”.

Will changes to the core requirement selection always be tied to a change in CSF versions?

Yes, a new major or minor CSF version will be released each time the core requirement selection changes.

Does v11 change the way that factors work to tailor an r2 assessment?

No, the r2 assessment factors continue to work in v11 just as they do in v9.x.

Are v11 r2 assessments larger than v9.x assessments?

No, the average v11 assessment is up to 9% smaller in requirement count compared to v9.x assessments (depending on the v9.x version used).