HITRUST Security and Compliance Self-Assessment

Introductory Webinar
What is the HITRUST security assessment?

What is HITRUST?

- HITRUST, the Health Information Trust Alliance, has established the Common Security Framework (CSF), a certifiable framework used by organizations that create, access, store or exchange personal health and financial information
- HITRUST CSF is the most widely adopted security control framework in US healthcare, developed in collaboration with healthcare, business, technology and information security leaders

What does the athena-HITRUST partnership look like?

- athena is partnering with HITRUST to provide a verified self-assessment for all MDP partners; partners will score themselves on the self assessment and HITRUST will perform a limited quality assurance review
- While athena is covering the costs associated with the initial assessment for all MDP partners, HITRUST is verifying the assessment independently
- MDP partners are responsible to work with HITRUST directly to complete the process
- Partner must start the process with HITRUST before going Generally Available (GA) on the Marketplace and must pass the process within 90 days of going GA to have their tile remain
What will the process look like?

Partner prepares for HITRUST process

Partner takes self assessment

HITRUST verifies self assessment

As needed: Partner responds to concerns

*Must be redeemed before going GA
**If QA materials are not submitted to HITRUST within 30 days of the request, an automatic fail will be issued by HITRUST
Preparing for the process

- Review any questions you have with your Onboarding Specialist (OBS)
- Partner prepares internal security and compliance materials
- Upon request of partner, OBS will provide a coupon code to be redeemed with HITRUST
Executing the self assessment

- Partner will start the self assessment process by contacting HITRUST (information on slide 10) and providing them with the coupon code given by the OBS.
- Partner completes all questions required in the self-assessment; varies from 199-592 questions.
- Partner must submit self assessment through HITRUST’s MyCSF portal (the self assessment home page), otherwise no further action will occur.
- From redemption of coupon, there are 90 days to complete the process in full.
Upon submission, HITRUST will select one control to audit

HITRUST will request materials for this section

Partner has 30 days to respond to the audit with their supporting documentation

If there is no response to the audit, the assessment will result in an automatic failure
• If HITRUST verifies your score with the audited materials, you will receive your final score report.

• Partner will then send the final Score Report to the OBS.

• If HITRUST fails the score compared to the audited material, the partner is required to retake the self assessment at their own cost.

• Partner is subject to be removed from the Marketplace if they do not pass.
Two results required from this process

1. **Score of 3- or higher**

   Score is based on the policies and procedures in place to ensure security along key CSF control areas.

   Partners receiving a score of 3- or higher have fulfilled their commitment to the athena HITRUST process*

   Partners receiving a score below 3- will have to implement corrective changes and re-take the assessment.

   *This alters from HITRUST’s standard scoring. HITRUST requires a score of 3 with Corrective Action Plans or a 3+ or higher for certification.

   *It is possible to have an individual control scored less than 3- and still achieve a passing overall score. A domain score less than a 3- would be an automatic fail.

2. **Pass verification rating**

   A pass rating will be issued by HITRUST if materials provided for the audited section support the self-assessment answers (i.e., self-assessment was filled out accurately and honestly).

   A Fail rating will be issued if partner can not provide supporting documentation for self-assessment or supporting documentation does not align with scores assigned; this includes proper dating and authorization on documentation.

   Partners receiving a Fail rating will have to re-take the assessment or risk removal from the Marketplace.

Please note that there are different scoring programs between HITRUST’s standard process and athena’s self-assessment program.
Two possible outcomes based on score

<table>
<thead>
<tr>
<th>Maturity Level</th>
<th>Evidence is in place to demonstrate that the organization:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 1-</td>
<td>Has an informal security program</td>
</tr>
<tr>
<td>Level 1</td>
<td>Relies on policies to enforce the majority of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 1+</td>
<td>Relies on policies to enforce all of the HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 2-</td>
<td>Has policies and supporting procedures and technologies that can be used to enforce some of the HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 2</td>
<td>Has policies and supporting procedures and technologies that can be used to enforce the majority of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 2+</td>
<td>Has policies and supporting procedures and technologies that can be used to enforce all of the HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 3-</td>
<td>Has policies and supporting procedures and technologies that are consistently used to enforce some of the HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 3</td>
<td>Has policies and supporting procedures and technologies that are consistently used to enforce the majority of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 3+</td>
<td>Has policies and supporting procedures and technologies that are consistently used to enforce all of the HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 4-</td>
<td>Routinely conducts tests to evaluate the adequacy and effectiveness of implemented controls for some of the HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 4</td>
<td>Routinely conducts tests to evaluate the adequacy and effectiveness of implemented controls for the majority of the HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 4+</td>
<td>Routinely conducts tests to evaluate the adequacy and effectiveness of implemented controls for all of the HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 5-</td>
<td>Consistently produces and actively monitors status metrics for the information security program as well as some of the individual HITRUST critical control areas and the individual controls apply to some of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 5</td>
<td>Consistently produces and actively monitors status metrics for the information security program as well as the majority of the individual HITRUST critical control areas and the individual controls apply to the majority of the systems within the assessment scope</td>
</tr>
<tr>
<td>Level 5+</td>
<td>Consistently produces and actively monitors status metrics for the information security program as well as all of the individual HITRUST critical control areas and the individual controls apply to all of the systems within the assessment scope</td>
</tr>
</tbody>
</table>

Note, this is at the domain level; an individual control can be less than a 3- in the athena program, but the overall score must be 3- or better

Partner required to implement changes and re-take HITRUST assessment

No further action required
How to get started

1. Designate internal lead responsible for leading assessment
   - Likely to be from security department, CTO’s office, network admin, etc.

2. Review resource materials provided

3. Call HITRUST to submit assessment code provided by athena and set up access to the online assessment portal
   - *It is important to note you will have 90 days of access to the portal in which to complete and submit the self-assessment. If not complete within 90 days notify athena and your access can be extended by 30 days. After this extension access can only be continued at a cost of $500/mo paid by the partner.
   - As needed, grant access to additional users (up to 5 total users) during initial phone call (at 469.269.1100) or by emailing sales@hitrustalliance.net

4. Create and scope the assessment for your organization
   - Complete **Organization Information**, **Systems**, and **Facilities** tabs
   - Select "**CSF Security Assessment**" in **Assessment Options** tab; select **Self-Assessment** (not validated)
   - Complete **Factors** tab (only select regulatory factors that apply to systems in scope)

5. Complete the assessment as directed
Where to go for help

**Check the resource materials provided** as a first resource for:
- Understanding assessment framework and scoring (see appendix slides 18 and 19)
- Guidance on completing the online assessment tool
- Creating a corrective action plan

**HITRUST**

Review the ‘Admin Tool’ in your MyCSF portal or e-mail [support@hitrustalliance.net](mailto:support@hitrustalliance.net) for questions related to:
- Registering users and accessing the online assessment tool
- Content related to the online assessment tool, including scoring
- Documentation needs for supporting self-assessment scores

**athena**

Email athena contacts for questions related to:
- Overall process and timelines
Partner to assign internal lead

Request sample resource materials from OBS
  Scoring Rubric and Sampling Guideline are noted in the Appendix

Partner to request coupon code when ready to start process
  (must be redeemed before going GA)
Appendix
Don’t select regulatory requirements without first discussing with athena – doing so will increase the workload required by the tool and may not be necessary given robustness of CSF framework.

Take care to define applications and facilities at the appropriate level of detail.

Go to MyCSF Assessments tab to look at current status of assessment (becomes read-only once submitted).

Within the assessment, Diary tab is helpful for internal notes (comments don’t appear in the report) and Assessor tab can be ignored as this is only used for validated assessments.
<table>
<thead>
<tr>
<th>Resource</th>
<th>Where to find it</th>
<th>What to use it for</th>
</tr>
</thead>
</table>
| Getting Started Guide    | https://hitrustalliance.net/content/uploads/2014/10/MyCSFGettingStartedGuide.pdf | • Guidance on online assessment tool  
• Instructions for completing assessment                                          |
| User Guide               | https://hitrustalliance.net/content/uploads/2015/02/MyCSFUserGuide.pdf          | • Detailed instructions on using online assessment tool and completing assessment   |
| Sample Assessments       | PDF and excel versions provided by athena team                                   | • Understanding assessment components  
• Viewing assessment components outside online tool                                   |
| Score Report             | Template provided by athena team                                                | • Understanding score report components  
• Guidance on Corrective Action Plan needs (recommendations included in report)       |
| MyCSF Library            | Tab accessible within CSF portal                                                 | • Detailed information on CSF framework and regulatory requirements                |
| Risk Analysis            | https://hitrustalliance.net/content/uploads/2014/10/RiskAnalysisGuide.pdf       | • General info on the HITRUST framework, assessment, and scoring rubric             |
| Risk Management Frameworks | https://hitrustalliance.net/content/uploads/2014/05/HITRUST-RMF-Whitepaper2.pdf | • High-level introduction to HITRUST framework and process  
• FAQs on HITRUST assessment                                                            |
Frequently Asked Questions (I)

What are the score standards based on?
The standards are based on the cut-offs HITRUST uses for its third-party certification process.

Does HITRUST outsource the audit?
No, HITRUST completes the audit and scoring internally.

Will athena see my full assessment?
HITRUST will not share your assessment with athena, but we will expect to see the score report, which includes some commentary on practices.

Can we submit another certification report in lieu of doing the HITRUST assessment?
No. In order to maintain consistency across the Marketplace and our partners, we must ensure all partners complete the same assessment.

What happens after I submit the assessment?
HITRUST will review the assessment, select one control to audit, and reach out to you to ask for supporting documentation.

How will the results be reported?
HITRUST will email both you and athena with its score report, which will also be available online via the portal.

How is the audited section selected?
It’s selected completely at random.

Is this the same as HITRUST certification?
No. HITRUST Certification requires a third-party assessor to perform all aspects of the assessment.
What happens after I submit the assessment?
HITRUST will reach out to you via email with next steps for the audit. If you haven’t heard from them after one week, please reach out to athena.

Can I calculate my score as I go?

How will athena get my score report?
HITRUST will inform both you and athena of the pass/fail status of the audit when it is complete. Following that, HITRUST will issue its assessment report to you, which you can then share with athena to confirm your completion of the process.
# Guide to selecting the right score

<table>
<thead>
<tr>
<th>Score</th>
<th>Policy</th>
<th>Procedure</th>
<th>Implemented</th>
<th>Measured</th>
<th>Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>0%</td>
<td>None of the CSF requirements</td>
<td>None of the CSF requirements</td>
<td>None of the CSF requirements</td>
<td>No measure or metric in place</td>
<td>No management action taken</td>
</tr>
<tr>
<td>25%</td>
<td>Some CSF requirements AND ad hoc</td>
<td>Some CSF requirements are supported by ad hoc procedures</td>
<td>Some CSF requirements AND partial scope</td>
<td>Operational OR independent measure</td>
<td>Measure or metric AND management actions are sometimes taken on an ad hoc basis</td>
</tr>
<tr>
<td>50%</td>
<td>All CSF requirements AND ad hoc</td>
<td>All CSF requirements are supported by ad hoc procedures</td>
<td>Some CSF requirements AND full scope</td>
<td>Operational AND independent measure</td>
<td>Measure or metric AND management actions are sometimes taken AND a formal action management process exists</td>
</tr>
<tr>
<td>75%</td>
<td>Some CSF requirements are written/signed AND the remainder ad hoc</td>
<td>Some CSF requirements are supported by written and/or automated procedures, AND the remaining CSF requirements are addressed by ad hoc procedures.</td>
<td>All CSF requirements and partial scope</td>
<td>Operational OR independent METRIC</td>
<td>Metric only AND corrective actions are always taken AND on an ad hoc basis</td>
</tr>
<tr>
<td>100%</td>
<td>All CSF requirements and written/signed</td>
<td>All CSF requirements are supported by written procedures and/or are automated</td>
<td>All CSF requirements AND full scope</td>
<td>Operational metric AND independent measure or metric</td>
<td>Metric only AND corrective actions always taken AND a formal remediation management process exists</td>
</tr>
</tbody>
</table>
Various Sampling Approaches

- Sampling should cover all objects of the in-scope environment
  - Sample should mix locations (if appropriate)
  - Three samples methodologies
    - Random - No structured technique (most unbiased method)
    - Systematic - Selecting every nth item
    - Haphazard - No structured selection technique

<table>
<thead>
<tr>
<th>Nature of Control and Frequency of Performance</th>
<th>Minimum Number of Items to Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manual control, performed daily or many times a day, population &gt;250</td>
<td>25</td>
</tr>
<tr>
<td>Manual control, performed weekly</td>
<td>5</td>
</tr>
<tr>
<td>Manual control, performed monthly</td>
<td>2</td>
</tr>
<tr>
<td>Manual control, performed quarterly</td>
<td>2</td>
</tr>
<tr>
<td>IT General Controls (ITGCs)</td>
<td>Same as guidance for manual controls above</td>
</tr>
<tr>
<td>Application Control</td>
<td>Can perform a test of one (test the application control once) where ITGCs are tested and determined to be effective; else test the application control 25 times</td>
</tr>
<tr>
<td>50-250 items in population</td>
<td>10%</td>
</tr>
<tr>
<td>&lt;50 and not weekly, monthly or quarterly</td>
<td>Use judgement, but consider selecting (5) items or test entire population</td>
</tr>
</tbody>
</table>
1. Reach out to your OBS/Marketplace Manager to discuss the result
2. OBS/Marketplace Manager will provide a second coupon code to redeem with HITRUST
3. Complete the self assessment again after addressing HITRUST’s concerns
4. Upon completion and a passing grade, forward the assessment report to your OBS/Marketplace Manager

• Partner to be invoiced the cost of the second coupon