

cloudticity

Demystifying HITRUST CSF v11

Learn what has changed and how it will affect your organization

Table of Contents

INTRODUCTION 3

WHY WAS CSF V11 CREATED? 4

WHAT HAS CHANGED WITH CSF V11? 6

- Traversable assessment portfolio 6
- Threat-adaptive controls 7
- Rapid recertification 8
- Broadened authoritative sources 8
- Clearer language 9
- Fewer requirement statements 9
- Continued inheritance 10
- Sunsetting older versions 10

HOW CAN CSF V11 BENEFIT YOUR ORGANIZATION? 11

NAVIGATE HITRUST CHANGES WITH CLOUDTICITY 13

INTRODUCTION

The new version of the HITRUST Common Security Framework (CSF) is here. In January 2023, HITRUST released CSF version 11, which includes substantial changes since the most recent previous version, 9.6. The updated version was designed to better address evolving cyber threats, incorporate new standards, and make it simpler for organizations to achieve higher levels of certification.

Unpacking the modifications to the framework can be challenging. But identifying key changes can help your organization better understand their potential benefits. For many organizations, moving to CSF v11 will help bolster security and improve compliance while streamlining the path to certification.



WHY WAS CSF V11 CREATED?

HITRUST continuously updates its framework to help ensure organizations sufficiently protect themselves from the newest cyber threats and adhere to the latest versions of standards. At the same time, HITRUST is committed to making it easier for organizations to provide assurances about security and compliance. CSF v11 was created to address all of these goals.

Protect against evolving threats

The healthcare industry is by far the most highly targeted industry by cybercriminals. Healthcare organizations must defend themselves against a growing number of threats and a rapidly evolving threat landscape.

HITRUST monitors shifting cyber threat trends and incorporates new information into the control requirements of its assessments through periodic updates. In CSF v11, HITRUST applies this adaptive approach to evolving threats across its entire assessment portfolio, helping to ensure that organizations protect against the latest threats no matter which assessment they use.

Incorporate new and refreshed standards

HITRUST certification provides verifiable compliance with a range of standards and regulations. But those standards and regulations can change frequently. Organizations such as the National Institute of Standards and Technology (NIST), for example, periodically update standards and issue new versions.

HITRUST CSF v11 incorporates new standards and refreshes the mappings between updated standards and control requirements. With v11, HITRUST intends to help organizations better assure partners and customers that they are adhering to the most recent versions of standards.

Streamline the journey to certification

Achieving HITRUST certification is not easy. Your organization might be required to demonstrate that you have hundreds of controls in place to protect data and comply with standards.

While conducting an assessment will always be a rigorous process, HITRUST wants to streamline the effort required for achieving certification. In particular, with CSF v11, HITRUST aims to make it simpler to move up from one level of certification to another. Your organization should be able to build on previous assessment and certification work as you further enhance security and compliance.



WHAT HAS CHANGED WITH CSF V11?

HITRUST CSF v11 has introduced several key changes that should enhance security, improve compliance, and accelerate assessments.

Traversable assessment portfolio

With v11, HITRUST has altered its assessment offerings in part to make its portfolio more "traversable"—that is, easier for organizations to move from lower-level to higher-level assessments and certifications. Lower-level assessments are now subsets of higher-level assessments, enabling organizations to leverage all their previous work as they move toward higher-level certifications.

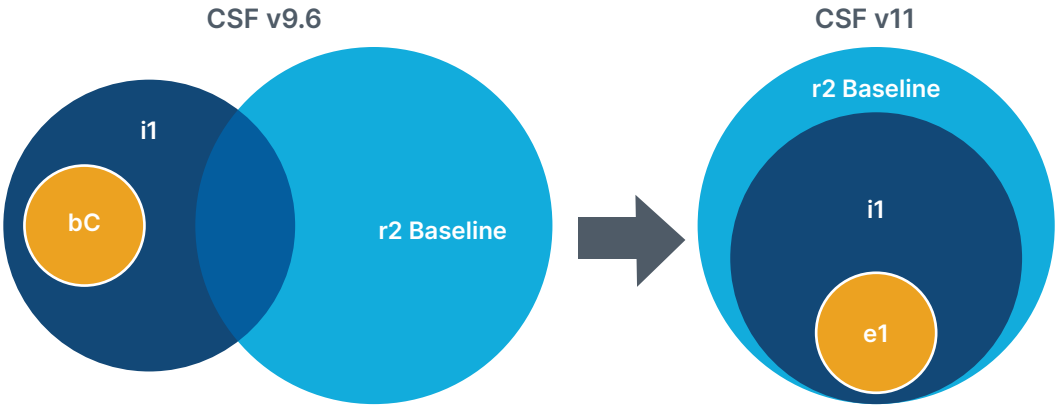
In making the assessments traversable, HITRUST has modified its offerings. The three current assessments include:

- **HITRUST Risk-based, 2-year (r2) Assessment:** The r2 assessment remains the most rigorous assessment, with the most comprehensive set of control requirements.
- **HITRUST Implemented, 1-year (i1) Assessment**: Initially introduced in 2021, the i1 assessment provides a moderate level of assurance that organizations have adequately addressed cybersecurity threats.
- **HITRUST Essentials, 1-year (e1) Assessment:** Newly introduced with CSF v11, the e1 assessment provides entry-level assurance that organizations have focused on the most critical cybersecurity controls and established essential cybersecurity hygiene. The e1 assessment replaces the HITRUST Basic, Current-state (bC) Assessment.

Previously, the three assessments offered by HITRUST had some overlapping control requirements, but not all lower-level requirements were included in higher-level assessments. Specifically, organizations that completed the i1 assessment would have discovered that not all of the controls put into place for that assessment could be reused for the r2 assessment.

With CSF v11, HITRUST ensures that the assessment levels are completely nested. All e1 requirement statements are part of the i1 assessment; and all i1 requirements are part of the r2 assessment. As a result, organizations can move much more swiftly and efficiently from a lower-level to a higher-level assessment.

i1 Requirement Statements are Traversable



All i1 requirement statementscare now part of the "Core" on an r2 assessment

With CSF v11, HITRUST modified its assessments so that the requirement statements for each lower-level assessment are contained within higher-level assessments.

Threat-adaptive controls

When the i1 assessment was introduced in 2021, HITRUST made it "threat-adaptive," meaning that it leverages continuously updated threat intelligence and integrates best practices that help protect against evolving cyber threats. This assessment was designed to stay current with new threats while retiring controls that are no longer needed.

With CSF v9.6, the threat-adaptive capabilities of the i1 assessment were not included with the r2 assessment. Now, with the nesting of the assessments in v11, the entire portfolio is threat-adaptive. The e1 assessment is threat-adaptive, and because e1 is part of i1 and r2, they too are threat-adaptive. Regardless of which assessment you select, your organization can benefit from this threat-adaptive approach.

Rapid recertification

CSF v11 introduces the i1 Rapid Recertification Assessment—an accelerated path for achieving i1 recertification. Instead of having to complete an entire i1 assessment every year, the i1 Rapid Recertification Assessment allows you to achieve recertification by demonstrating that your control environment has not materially degraded since the previous, full i1 assessment was performed. You can use this recertification process every other year, between full i1 assessments.

To achieve rapid recertification, you submit a sample of 60 requirement statements from the last full assessment. As long as only two or fewer scores have been lowered, you can continue with the rapid recertification. There are a number of additional rules and caveats with this recertification process, but overall, it provides an important means to simplify the recertification process. Your organization can save substantial time and effort in achieving an i1 certification.

Broadened authoritative sources

The HITRUST CSF maps requirements from key standards, or "authoritative sources," to specific controls. With CSF v11, HITRUST has added two new authoritative sources: the NIST SP 800-53 Rev. 5, and Health Industry Cybersecurity Practices (HICP) standards. Organizations that achieve certification can signal their compliance with more standards to partners and customers.

With CSF v11, HITRUST has also refreshed mappings to several sources, including:

- NIST SP 800-171
- NIST Cybersecurity Framework
- HIPAA Security Rule, Privacy Rule, and Breach Notification

Refreshing the mappings helps to ensure alignment with changes in the sources while also improving mapping efficiency. In some cases, HITRUST reduced the number and complexity of requirements—without jeopardizing compliance.

CSF v11 was the first release to use natural language processing technology to assist with mapping. This AI-based technology supplements the NIST Online Informative References (OLIR) program methodology, which defines mapping type and strength. Using natural language processing improves the efficiency of the mapping process, which should enable HITRUST to add new authoritative sources faster in the future. At the same time, this technology should help HITRUST reduce the number of elements that must be assessed: For your organization, that could mean less effort to comply with standards and regulations.

Clearer language

Previously, the "evaluative elements"—the criteria that organizations must meet to comply with a requirement—were often difficult to decipher. These elements were contained in the policy "illustrative procedures," which provide assessment guidance. But the elements were found within a large body of text.

With CSF v11, HITRUST has moved those evaluative elements to the requirement statement. And importantly, HITRUST has broken the text into numbered statements that are better formatted for readability. HITRUST also updated the illustrative procedures for clarity, using more concise wording. As a result, it's easier to understand each requirement and conduct assessments.

Fewer requirement statements

CSF v11 has reduced the number of requirement statements in the i1 and r2 assessments. For example, the i1 assessment previously had 219 requirement statements; with CSF v11, it has 182. Refreshing the authoritative source mappings, using threat-adaptive capabilities, nesting assessments, and conducting additional consolidation work all have contributed to the reduction of requirement statements. These reductions enable you to achieve certification faster and with less effort than before.

Continued inheritance

To speed the journey to certification, organizations often “inherit” compliance controls from HITRUST-certified cloud and managed service providers. In other words, once your organization has determined which controls you must attest to, you do not have to implement controls that your certified cloud or managed service provider has already covered.

The ability to inherit controls from external organizations continues with CSF v11. Of course, if your cloud or managed service provider is still using CSF v9.x, some inherited controls might no longer be applicable with v11.

Sunsetting older versions

With the introduction of CSF v11, HITRUST will begin gradually retiring older CSF versions. But that sunsetting process will be very gradual, giving all organizations sufficient time to transition to the new version.



HOW CAN CSF V11 BENEFIT YOUR ORGANIZATION?

CSF v11 should deliver some important benefits for healthcare organizations.

Better security

HITRUST is committed to tracking changes in cybersecurity and modifying control requirements to help organizations better protect themselves from evolving threats. By nesting the three assessment levels, HITRUST has made sure that every assessment incorporates that continuous threat monitoring work. As a result, organizations that pursue HITRUST certification, at any level, will gain the guidance for securing data and defending against new threats.

Stronger compliance

By adding new authoritative sources and refreshing mappings to existing sources, CSF v11 helps ensure that organizations comply with a broader range of key standards and adhere to the latest versions of those standards. Consequently, when your organization achieves HITRUST certification, you can give your partners and customers greater assurance that you are fully complying with applicable regulations and standards.

Streamlined assessment and certification

CSF v11 should make it easier to achieve certification. The new e1 assessment, which replaces the bC assessment, offers an entry-level approach to achieving certification. There are only 44 requirements that need to be met.

With v11, it's also simpler to move up from one level of certification to another. You can start with an e1 certification and move up to an i1 assessment while preserving the work you've already done. Similarly, you can move from an i1 to an r2 assessment without wasting any of your completed work.

If you achieve i1 certification, the i1 Rapid Recertification Assessment lets you recertify much faster and with much less effort than going through the full certification process. You can maintain the same level of i1 certification while assessing only a fraction of the requirements needed for a full assessment.

Additional modifications introduced with CSF v11—from the changes in how requirements are conveyed to reductions in the number of requirement statements—should reduce the effort for conducting assessments. Meanwhile, the continued ability to inherit controls help ensure that your organization can continue to benefit from time-saving inheritance in the future.

Competitive advantage

Earning HITRUST certification can help your organization gain a competitive advantage in the healthcare industry. Certification puts you in a select tier of companies. You can quickly gain the trust of partners and customers, and accelerate sales cycles by eliminating the need for extra security checks. Enhancements to CSF v11 should help that certification increase your competitive differentiation while also enabling you to achieve certification faster.

NAVIGATE HITRUST CHANGES WITH CLOUDTICITY

Changes to the HITRUST framework have the potential to deliver important benefits to healthcare organizations. Still, navigating all these changes can be difficult, especially for businesses that want to concentrate resources on innovation rather than assessment and certification work.

Cloudticity can help you determine how changes to the HITRUST framework will affect your particular organization. We can then develop a plan for adopting the new framework so that you can make the most of the changes without excessive effort. Working with Cloudticity, your organization can speed HITRUST certification and simplify ongoing certification while staying focused on innovation.

To learn more about what CSF v11 will mean for your organization and to start planning your move to the new framework, speak to a healthcare cloud expert at Cloudticity.


cloudticity
Meet with an Expert and Map Out Your HITRUST Journey Today!
SCHEDULE A HITRUST CONSULTATION