HITRUST®

Streamlining the Sharing of Assessment Data with HITRUST Inheritance

What is Inheritance?

HITRUST® inheritance streamlines the assessment process by saving organizations time and money that would have otherwise been spent on duplicative testing and enabling access to testing results that may have otherwise been unavailable. The HITRUST MyCSF® platform's inheritance functionality enables the importing of PRISMA-based control maturity scores and associated commentary present in another validated HITRUST CSF® assessment. The validated HITRUST CSF assessment from which scoring and commentary are inherited can belong to your own organization, one of your service providers, or one of their sub-service providers.
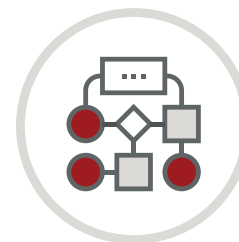
Key Benefits
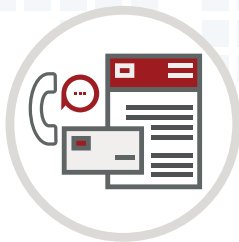
Facilitates the collection of detailed information about the performance of controls in a service provider's environment.

Eliminates the manual hand-off of third-party assurance reports.

Reduces duplicative assessment testing and data entry.

Internal Inheritance

Assessing the entirety of your organization's control environment can be a large undertaking; many organizations prefer to segment their environment and perform multiple, smaller assessments rather than assess all information risk management and compliance measures at once. Due to the comingled nature of an organization's control environment, the same controls can appear in multiple assessments performed across a single organization. Internal inheritance enables an organization to rely upon their own previously completed testing, eliminating the need for duplicative testing and/or duplicative documentation.

For example, an organization may first choose to perform a HITRUST CSF Validated Assessment that includes primarily entity-level controls. This assessment would include controls that, for the majority of entities, are applicable across the entire organization (such as those pertaining to personnel security or awareness training). After the report is finalized, they may choose to perform a second assessment against a separate part of the organization that also utilizes those entity-level controls. The applicable testing results from the first assessment could easily be inherited into the assessment currently being performed with no need to re-score, rewrite comments, re-test, or re-validate.

External Inheritance

The increased reliance on hosting, cloud, and service providers has created new challenges in the risk management and compliance landscape. Organizations utilizing service providers are faced with the responsibility of ensuring that their sensitive data is protected—regardless of how that data is stored or who may have access. External inheritance enables service providers to make their HITRUST CSF Validated Assessment results available through MyCSF for seamless integration into any of their customers' assessments. This simplifies assessment processes by reducing the manual hand-off of assessment results between service providers and their user organizations and allows service providers the ability to manage the sharing of assessment data holistically rather than on an individual basis.

The MyCSF platform has the ability to serve as a means of determining what controls are inheritable, validating the applicability of inheritance requests to the scope of the assessment, orchestrating the exchange, and managing the process. This dramatically reduces the level of effort for all involved. By working with a participating service provider, customers can reduce the required testing and associated costs for inherited controls in a fully automated manner. With external inheritance, organizations of all sizes and levels now have the ability to leverage cloud platforms to their utmost potential because HITRUST has worked with service providers to accept responsibility (either in full or shared) for delivering on many security control objectives on behalf of their tenants. This gives customers and service providers a complete understanding of which parties are responsible for which controls.

Partial Inheritance

In some cases, responsibility for a single control may be shared between multiple parties. For example, an organization using a hybrid cloud environment may host a portion of their servers on-premise and the remainder with a cloud service provider. Through partial inheritance, the assessed entity can assign a weighted percentage for each control in question. MyCSF then averages the scores from the service provider's control maturity levels and those of the organization inheriting the control.

Additionally, the introduction of the HITRUST Shared Responsibility Matrices gives tenants coverage for an infinite number of combinations of real-world delivery models in which the distribution of labor and responsibility is customizable to their needs rather than being forced into one of a handful of deployment models.

Requirements

The following requirements must be met in order for inheritance from another validated HITRUST CSF assessment to occur (all of which are automatically enforced by or enabled through MyCSF):

1. A valid basis must exist for the inheritance. For example, it would be inappropriate to inherit from a service provider that does not actually provide services relevant to the scope of the assessed entity's validated assessment.

2. The original HITRUST CSF Validated Assessment (e.g., Host CSP or parent organization's assessment) must be completed with the final report posted in MyCSF.

3. When performing External Inheritance, the original HITRUST CSF assessment object must be configured to allow inheritance. The organization holding that HITRUST CSF assessment must hold either a Corporate or Premier MyCSF subscription level in order for their assessment object to be inheritable.

4. The original HITRUST CSF Letter of Certification must be dated less than two years prior to the inheritance, and the Interim Assessment must have been successfully completed prior to the one-year anniversary of the date on the letter of certification. If the assessment did not achieve certification and is a HITRUST CSF Validated Assessment Report, the HITRUST CSF Letter of Validation must be dated less than one year prior to inheritance. Obtaining a HITRUST CSF Bridge Certificate does not extend these expiration dates.

5. Both the assessed entity and the organization holding the HITRUST CSF Assessment Report must agree to share the pertinent assessment information with one another (e.g., the control requirement statements with the PRISMA-based control maturity scores that will be inherited and associated commentary).

Leveraging the inheritance features of MyCSF, in conjunction with the Shared Responsibility Program and Matrices, can help significantly reduce efforts for both service providers and their customers. To learn more about leveraging these tools, contact sales@hitrustalliance.net.