HITRUST®

Addressing Vendor Risk & Assurance Challenges in the Cloud

FAQs

Q: As a Software as a Service (SaaS) cloud vendor, how should we give our customers a greater level of comfort over our data security practices if our existing compliance reports (HIPAA, HITRUST®, SOC 2, PCI, etc.) do not appear to be sufficient?

A: As a SaaS cloud vendor, it is incumbent to demonstrate the effectiveness of the controls in place governing the security practices over protecting and handling customer-entrusted data. This can be achieved through various levels of transparency by sharing compliance reports; however, there remain concerns over a disconnect regarding expectations or uncertainty of how that security control responsibility should be shared. For SaaS cloud vendors with a HITRUST CSF Certification, there is the opportunity to publish a a cloud service provider (CSP)-specific HITRUST Shared Responsibility (SR) Matrix™ relative to their service offerings that inform customers (or prospective customers) with a greater level of transparency of the comprehensive set of security/privacy/risk management controls as well as provide clarity over how responsibility is shared based on a common industry standard adopted by leading CSPs.

Q: How do organizations handle the situation when CSPs hosting their applications only permit their customers to review their SOC 2/SOC 3 reports instead of performing an audit?

A: It is becoming more common practice for CSPs to significantly limit or entirely restrict customer audits as they are often impractical, with the risks of business disruption or exposure that could breach other tenants' security requirements. For this reason, HITRUST offers the ability for customers to obtain a HITRUST CSF Assessment and inherit applicable control requirement statements and associated assessment result scores from HITRUST CSF Certified CSPs. For more information, read our datasheet or peruse the HITRUST MyCSF® User Guide. Alternatively, if not yet pursuing a HITRUST CSF Assessment, the published cloud CSP-specific HITRUST SR Matrix can serve as an informative vendor risk assessment tool, detailing the comprehensive set of security/privacy/risk management controls relative to the CSP's service offerings as well as clarity over how responsibility is shared based on a common industry standard adopted by leading CSPs.

Q: How is the HITRUST CSF® framework maintained to ensure it accounts for current/emerging threats? What sources are used for threat information?

A: HITRUST maintains an ongoing partnership with Cysiv. Whenever presented with new, emerging threats, the HITRUST Standards team ensures that there are controls within the HITRUST CSF to adequately address these threats; if not, new controls are added to the framework. The HITRUST Threat Catalogue™ helps organizations align the most common threats in their environments to controls within the framework that address those threats.

Q: If a client uses a CSP and the HITRUST Authorized External Assessor needs to verify a specific control requirement statement, such as that the CSP has fire extinguishers every 50 ft in their data center, how does the assessed entity get that data via inheritance?

A: There is a functionality within MyCSF available to annual subscribers that allows for an assessed entity to import data for applicable control requirement statements and associated assessment result scores from service providers into their own assessments, referred to as inheritance. For more information, read our datasheet or peruse the MyCSF User Guide.

Q: Is there a different type of MyCSF subscription that allows access to the controls available for inheritance? If so, would they have access to all allowable shared statements?

A: All annual MyCSF subscriptions allow for inheritance and can inherit data from any applicable service provider that is participating in the inheritance program (pending approval from the service provider). For more information, read our datasheet.

Q: Is there a list of CSPs that are using the HITRUST SR Matrix and supporting the inheritance functionality?

A: HITRUST does not publish the list of service providers participating in the inheritance program. However, as a MyCSF subscriber performing a HITRUST CSF Assessment, the list of participating service providers is made available as part of the external inheritance request process for any particular control requirement statement. Further, CSPs participating in the inheritance program will have the option to publish a CSP-specific HITRUST SR Matrix available for download from the HITRUST website.

Q: Is the SR Matrix available to all levels of annual MyCSF subscription (Professional, Corporate, and Premier)?

A: There are two versions of the HITRUST SR Matrix with the shared responsibility model (SRM) baseline inheritance template available for download: a control summary version, which is included with the HITRUST CSF framework download, and a full version, accessible to all MyCSF subscribers. The CSP-specific HITRUST SR Matrices published on the HITRUST website will be available for public download (subject to accepting HITRUST's end-user licensing terms).

Q: If a client's CSP is not HITRUST CSF Certified and the client outsources everything to that vendor, how does the External Assessor address the Policy and Procedure scoring?

A: Guidance as to how to score these control requirement statements can be found in the HITRUST CSF Assurance Program Requirements document. Remember that customers can outsource implementation but cannot outsource accountability. CSPs can and should have policy, but it is up to the assessed to have it's own policies and ensure alignment.

Q: When will HITRUST CSF v10 be published?

A: HITRUST CSF v10 will be available Q1 2021.

Q: If AWS, GCP, and Azure don't have specific HITRUST SR Matrices yet, then how can companies currently (let's say they are going through a validated assessment now) "inherit" those applicable requirement statements from the CSP?

A: Inheritance is already an existing function of the MyCSF platform. CSP-specific HITRUST SR Matrices merely take that to the next level and enable CSPs to manage inheritance requests collectively. All three have CSP-specific HITRUST SR Matrices in the final stages of production.

Q: Is the SR Matrix a guide that is available outside of MyCSF or is this functionality built in?

A: There are two different versions of the HITRUST SR Matrix Template available: a control summary version, included with the HITRUST CSF framework download, and a full version, available within MyCSF. For more information about these matrices, see our datasheet.

Q: If an organization is being assessed on HITRUST CSF v9.3 currently, how does the release of v10 impact the Interim Assessment?

A: Interim Assessments are created using the framework version on which the original assessment was performed, so future releases of the framework will not impact Interim Assessments in any way.