Accelerate Your HITRUST® Journey Through Inheritance

Your HITRUST® Certification Journey Starts Here

Perhaps one of your biggest customers requires certification. Maybe your leadership team understands that HITRUST certification is the best way to demonstrate you are taking the most proactive approach to cybersecurity, data protection, and risk mitigation. Whatever the reason, you may be wondering where to get started and whether you can streamline some of the steps that lie ahead. Understanding Inheritance is a great place to start.

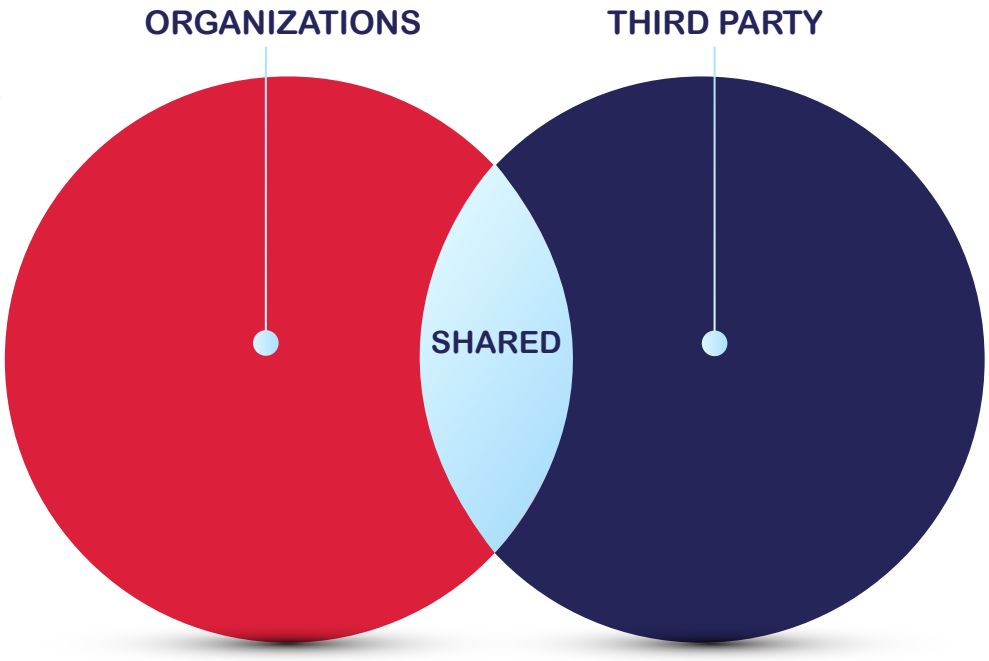
What is the HITRUST® Shared Responsibility and Inheritance Program?

The HITRUST Shared Responsibility and Inheritance Program lets organizations use already certified controls. Organizations can share information protection controls from internal shared IT services and external third-party organizations. These include service providers, vendors, and Cloud Service Providers (CSPs) like Amazon, Google, and Microsoft. The great news is that major CSPs already have HITRUST certifications. This makes it easier for organizations to achieve their certifications as they benefit from already certified controls from their CSP.

The HITRUST Shared Responsibility and Inheritance Program can help your organization save time and resources by identifying inheritable controls within the HITRUST CSF and streamlining security certification journeys.

What are Shared Responsibility Models?

You may have heard of various Shared Responsibility Models that major CSPs follow. As the name suggests, when an organization moves its data to the cloud, both the CSP and the organization share responsibility for its security.



In some security domains, the organization and the CSP have sole responsibility for different aspects of security without any overlap. For instance, CSPs are fully responsible for the physical security of their data centers. However, the lines between who is responsible for security controls aren't nearly as black and white. Many security controls involve shared responsibility for performance. For instance, cloud providers and customers often share responsibility for the identity and access management of cloud-based solutions.

The HITRUST® Shared Responsibility Model

Fully Inheritable

- Third-party service provider/data processor-only compliance
- CSP's on-premises data center security protocols
- Environmental protections not involving Tenant
- On-premises hardware/digital assets only accessible by CSP personnel

Partially Inheritable (within Tenant's cloud-hosted environment)

- Tenant's compliance with CSP's on-premises data center security protocols
- Subset of technologies and digital assets only accessible by CSP personnel
- Tenant's involvement in CSP's security, availability incident response processes, cloud service contracting, and SLAs
- Tenant's unfettered operation of purchased cloud services
- CSP's shared privacy regulatory compliance

Not Inheritable

- Tenant's organizational programs, policies, and procedures
- On-premises hardware/digital assets only accessible by Tenant personnel
- CSP remains fully responsible for independent compliance

What is the HITRUST Shared Responsibility Matrix?

Built upon the HITRUST CSF, the HITRUST Shared Responsibility Matrix (SRM) offers a commonly accepted shared responsibility and control analysis between CSPs and organizations.

It is a free, easy-to-use baseline template that pre-populates shared responsibility and controls inheritability, perfectly suited for shared cloud environments. The SRM simplifies and clarifies the practical application of control sharing. It is also available in tailored CSP-specific versions.

Benefits To Your Organization's HITRUST® Journey

Clarity

The HITRUST Shared Responsibility and Inheritance Program offers a simple methodology and a standardized structure that clearly defines who owns the different cloud security controls. It helps avoid confusion and ambiguity in cloud environments.

Transparency

Inheritance is transparent and easily accessible. It is commonly adopted by major CSPs and their users. This enables organizations to quickly understand and efficiently inherit existing control assessment data.

Time and Cost Savings

With inheritance from prior HITRUST assessments, your efforts are streamlined. Organizations can inherit as much as 65 – 85% of requirements in HITRUST assessments from participating CSPs. This depends on factors such as HITRUST CSF version, assessment type, and assessment tailoring. It eliminates redundancy and helps you save time and money while on the certification path.

Efficient Risk Management

The HITRUST Shared Responsibility and Inheritance Program facilitates efficient cyber risk management. Organizations can have seamless communication with CSPs and other vendors to align understanding and logistics to share controls equitably.

What is HITRUST® Control Inheritance?

Inheritance allows you to effectively manage ongoing assurances and demonstrate cyber maturity in protecting sensitive information.

When performing HITRUST assessments, Inheritance optimizes the use of prior HITRUST Validated or Certified Assessment results along with reliance on sharing cloud controls. Inheritance workflows within MyCSF allow organizations to import control assessment results and scores from the HITRUST assessments belonging to their internal and external service providers.

How Inheritance Works

From creating to validating and reporting, Inheritance offers smooth integration into the end-to-end assessment process.

Inheritance is done through MyCSF, HITRUST's SaaS tool used to perform controls assessments against the HITRUST CSF.

It extracts control data like statements and results from previously performed assessments and places them into the new assessment.

Inheritance automates the calculation of inherited control maturity scores and thus makes the exchange of assessment information seamless.

The Two Types of Inheritance HITRUST Supports

Internal

Organizations can inherit and repurpose their past control assessment results and scores via Internal Inheritance. When organizations reuse all or part of existing assessment results, it allows centralized and decentralized business functions to scope control environments into smaller sub-divisions.

This allows organizations to complete targeted assessments incrementally without including them all at once.

External

Using External Inheritance, organizations can import control assessment results and scores from other assessments belonging to their hosting, cloud, or other service providers. Approval workflows ensure that the service provider authorizes the assessment result sharing.

HITRUST

The HITRUST Shared Responsibility and Inheritance Program offers several benefits to accelerate your certification path.

https://hitrustalliance.net/shared-responsibility-and-inheritance-program