Maximizing Efficiency in HITRUST Assessments with Inheritance

HITRUST®

Getting Started with Your HITRUST Certification

One of your key customers requires certification, or your leadership team recognizes that HITRUST certification is the best way to demonstrate a proactive approach to cybersecurity, data protection, and risk mitigation. Whatever the reason, you may be wondering where to begin and how to make the process more efficient. Inheritance is a great place to start.

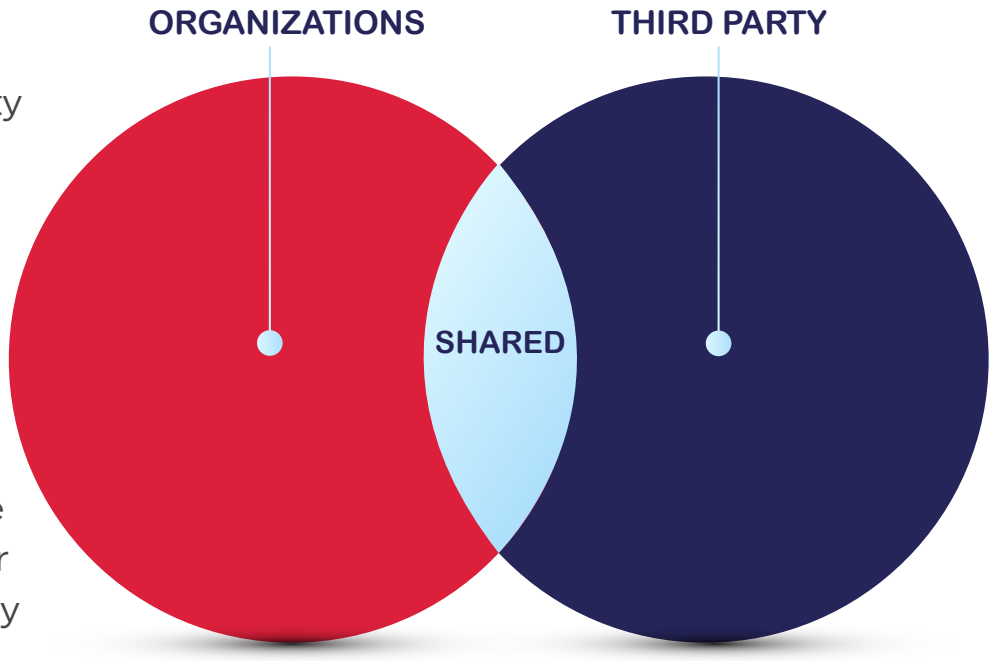
What is the HITRUST Shared Responsibility and Inheritance Program?

The HITRUST Shared Responsibility and Inheritance Program allows you to demonstrate security features from Cloud Service Providers (CSPs) like Amazon, Google, and Microsoft, using their HITRUST Validated Assessment Results.

The HITRUST Shared Responsibility and Inheritance Program reduces effort by applying your CSP's HITRUST assessment results to your own. Inheritance improves assurance, streamlines compliance efforts, and minimizes the workload required to demonstrate compliance.

What are Shared Responsibility Models?

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



For many controls, your organization and your CSP have sole responsibility for different aspects of security without any overlap. For instance, CSPs are fully responsible for the physical security of your data centers. However, the lines between who is responsible for security controls isn't always so black and white. For instance, CSPs and customers often share responsibility for the identity and access management. As an example, you likely configure the password length on your cloud console, and the cloud provider enforces that configuration.

The HITRUST Shared Responsibility Model

Fully Inheritable - These controls are fully managed by your CSP and already validated, you don't need to implement or test them, reducing compliance effort, audit scope, and assessment costs.

- CSP's compliance and physical data center security protocols
- CSP's environmental protections (not involving your team)
- CSP-managed on-premises security controls

Partially Inheritable (within your cloud-hosted environment) - You can leverage your CSP's assessment results, but you still need to demonstrate implementation within your environment, requiring some documentation and auditor review.

- Your compliance with CSP's security protocols
- Shared responsibility for security incident response processes
- CSP's shared privacy regulatory compliance

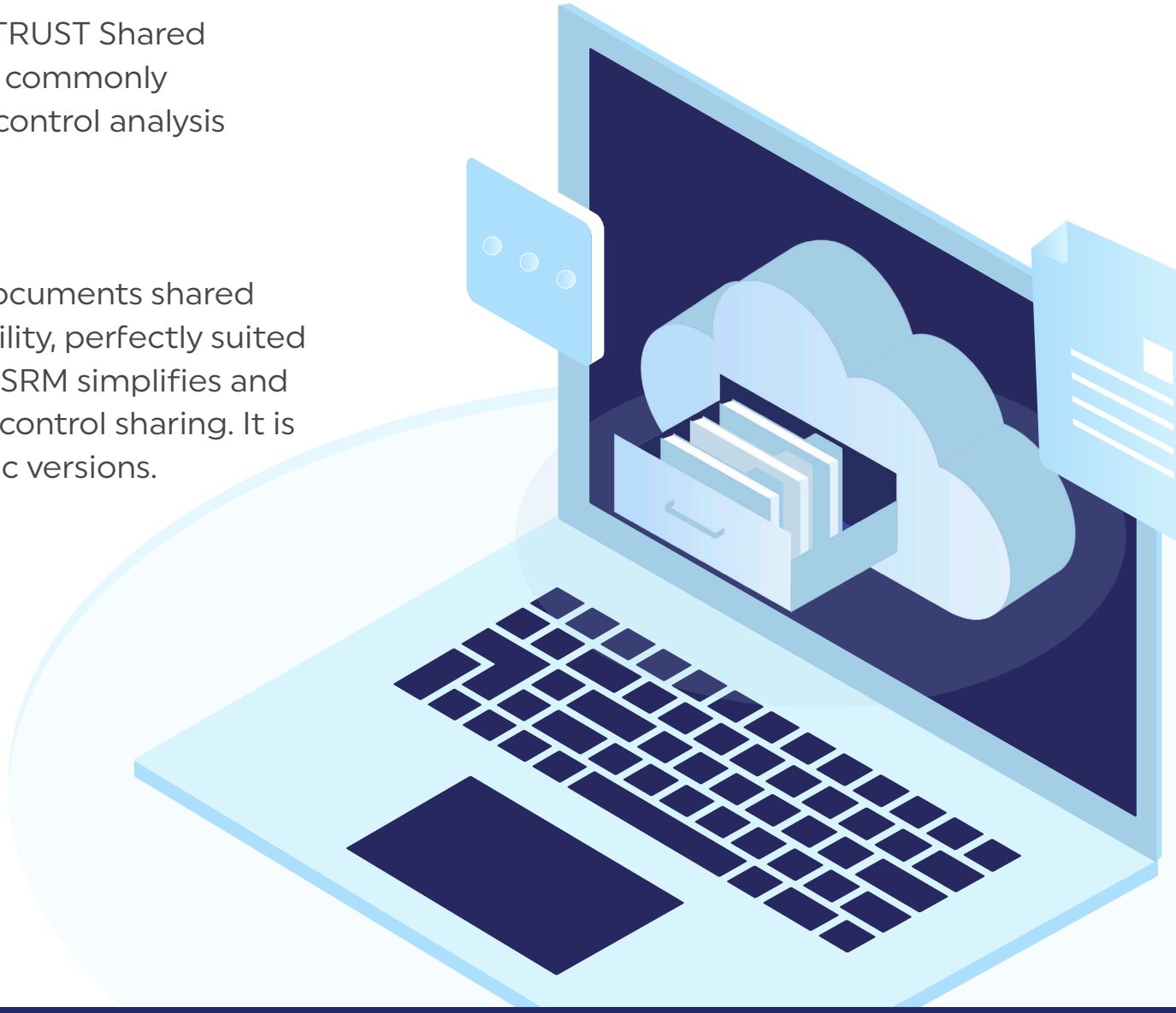
Not Inheritable - These controls are entirely your responsibility, requiring full implementation, documentation, and assessment, making them the most effort-intensive.

- Your internal security policies and procedures
- Your independent risk management process
- CSP's independent compliance obligations

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 their customers.

It is a free baseline template that documents 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.



Unlocking the Benefits of HITRUST Inheritance

Clarity

The HITRUST Shared Responsibility and Inheritance Program provides a standardized framework for defining control ownership, making it easier for you to demonstrate compliance. It helps you clearly understand which security controls you are responsible for and provides assessors with a structured way to evaluate compliance.

Transparency

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

Time and Cost Savings

You may be able to inherit as much as 65–85% of HITRUST assessment requirements from participating CSPs, depending on factors such as the HITRUST CSF version, assessment type, and tailoring. By leveraging existing validated controls, you can minimize redundant work, reduce audit scope, and lower compliance costs.

Efficiently Demonstrate Security

The HITRUST Shared Responsibility and Inheritance Program helps you efficiently manage cyber risk and demonstrate security posture by aligning with CSPs and vendors to share validated controls. However, your organization remains fully accountable for managing your own risk, ensuring compliance, and addressing gaps where inheritance does not apply.

What is HITRUST Control Inheritance?

Inheritance is an efficient approach to demonstrating the security of your system's cloud infrastructure.

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 you to import control assessment results and scores from the HITRUST assessments.

How Inheritance Works

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

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

Inheritance aligns assessment results with the results from your cloud service provider's HITRUST Assessment.

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

The Two Types of Inheritance

Internal

You can inherit and repurpose current assessment results via 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 assessing them all at once.

External

Using External Inheritance, you can import control assessment results and scores from your 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 streamline your certification path.

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