INTRODUCTION: The HITRUST Shared Responsibility Matrix™ Version 1.0

In 2018, HITRUST launched the Shared Responsibility (SR) Program as a strategic business priority to address growing misunderstandings, risks, complexities, and assurance inefficiencies when leveraging cloud service providers (CSPs). The primary objectives of the SR Program are to help clarify roles and responsibilities regarding ownership and operation of security and privacy controls shared with CSPs, and to support automation and streamlining of the assurance process when inheriting controls. With support from our SR Working Group of industry experts, the first major milestone has been met with the Version 1.0 general availability release of the HITRUST Shared Responsibility (SR) Matrix, with full cross-compatibility support for HITRUST CSF® Versions 9.1, 9.2 and 9.3.

This first release includes two versions for download: 1) a publicly-accessible control summary version which is now included in the HITRUST CSF Version 9.3 download package, and 2) a subscriber-only full version which can be downloaded via the new "References" landing page within the HITRUST MyCSF® portal.

The following table provides tab-specific information and features associated with the two versions of the SR Matrix:

Tab Name	Purpose	Control Summary Version	Full Version
Introduction	Introduction to the SR Matrix and what to expect after the V1.0 release.	✓	✓
License Agreement	SR Matrix V1.0 terms of use license agreement.	✓	✓
Shared Responsibility Model	Industry-guided HITRUST model used to build the SR Matrix which is comprised of a standard set of core principles and a common taxonomy with objective-based rationales and cloud use-case scenario assumptions/parameters to support shared responsibility claims and assertions.	✓	✓
HITRUST CSF® V9.x Matrix	Full forward/reverse cross-HITRUST CSF version compatibility, at the control requirement statement level, allowing for translation of external inheritance involving differing HITRUST CSF versions.	✓ *Note: Excludes underlying control requirement statement level detail*	✓
V9.x Control Summary	Summary view of the SR Matrix at the control-level, including a hyperlink feature to quickly jump into the control-specific shared responsibility value details contained within the HITRUST CSF® V9.x Matrix allowing for deeper analysis.	✓	✓
V9.1 CSP Matrix Template V9.2 CSP Matrix Template V9.3 CSP Matrix Template	SR Matrix template which can be customized by any SaaS, PaaS, IaaS, or Colo provider pre-populated with the default values pulled from the HITRUST CSF® V9.x Matrix to minimize ramp-up time.	✗	✓
V9.1 Control Summary V9.2 Control Summary V9.3 Control Summary	Summary view of the SR Matrix at the control-level, including a hyperlink feature to quickly jump into the control-specific shared responsibility value details contained within each of the V9.1, V9.2 & V9.3 CSP Matrix Templates allowing for deeper analysis.	✗	✓

What to expect next coming from the HITRUST Shared Responsibility Program…

Upon release, HITRUST is collaborating with the CSP community to support early adopters to manually generate their customized versions of the SR Matrix templates suited for their cloud service offerings. Meanwhile, cloud tenants now also have a new toolkit to help broker meaningful supplier risk conversations with their cloud-hosting providers. In turn by putting theory into practice, the following will be accomplished for the next series of roadmap offerings, planned for Q2-Q3 2020:

a) Implement SR Matrix feature enhancements, e.g., add automation that enables ease-of-use and shorter ramp-up time; and
b) Create a sustainable model to permit CSP to safely disclose their customized SR Matrices with their tenants upon request.

HITRUST will then partner with assessors and their clients to apply the SR Matrix as part of the assessment process. The lessons learned from the pilot will be an input to the next phase of maturation, advancing the SR Program through year-end by:

a) Building out new operational capabilities that uplift the HITRUST CSF Assurance and External Inheritance Programs supported by HITRUST MyCSF tooling automation enhancements; and
b) Providing input on control design and revision in the development of HITRUST CSF Version 10 to ensure clarity is sufficient when sharing security and privacy responsibility in the cloud.

Shared Responsibility Model

Not Inheritable	The design and operating effectiveness of the control is ***not reliant*** upon involvement from the cloud service provider (CSP) having influence over the suitability of the tenant's adoption and use of or access to the cloud services included in the HITRUST assessment scope boundary, such that, the tenant has full responsibility to: a) Implement organizational programs, policies and processes that may dictate or guide the suitability of the tenant's adoption and use of or access to the cloud services or; b) Implement security or privacy measures for a subset of technologies and/or facilities wholly controlled and operated by the tenant within the tenant's instance of an off-prem cloud-hosted environment. IMPORTANT: The CSP is still fully responsibility for independent compliance, and upon request, capable of assuring their tenants that these controls are suitably designed and remain in effective operation.
Partially Inheritable	The design and operating effectiveness of the control is ***partially reliant*** upon involvement from the cloud service provider (CSP) having influence over the suitability of the tenant's adoption and use of or access to the cloud services included in the HITRUST assessment scope boundary, such that, the tenant has full responsibility to: a) Implement organizational programs, policies and processes that may dictate or guide the suitability of the tenant's adoption and use of or access to the cloud services or; b) Implement security or privacy measures for a subset of technologies and/or facilities wholly controlled and operated by the tenant within the tenant's instance of an off-prem cloud-hosted environment.
Fully Inheritable	The design and operating effectiveness of the control is ***fully reliant*** upon involvement from the CSP having influence over the suitability of the tenant's adoption and use of or access to the cloud services included in the HITRUST assessment scope boundary, such that, the CSP has full responsibility to implement security or privacy measures for a subset of technologies and/or facilities wholly controlled and operated by the CSP within the tenant's instance of an off-prem cloud-hosted environment.

Shared Responsibility (SR) Matrix Template – Scoping Assumptions & Parameters

1. While the value of the HITRUST Shared Responsibility Model is that it can be applied to any type of security or privacy control as well as any form of cloud-hosted application or IT workload that may involve numerous CSPs; for sake of simplicity, the default inheritability values contained within the SR Matrix Templates are based on a more general use-case scenario that can be expanded upon when applied in practice, such as the following:

   a) It is assumed that the tenant is consuming cloud services from only one other third party offering SaaS, IaaS, PaaS or Colo public cloud services; and

   b) The CSP's control responsibility is independent from any managed service offering, such as those offered by security solution providers, to disregard the edge use-case scenario whereby the tenant has delegated a higher level of control responsibility to the CSP which is serving as an agent to enable the tenant's control capabilities.

2. The CSP may have ***full responsibility (or full control inheritability)*** for control compliance designed for and/or directed at third party suppliers and service providers.

3. The CSP may have ***partial responsibility (or partial control inheritability)*** to ensure the tenant is informed of their shared responsibility for physical access security, mobile device usage, and/or hardware equipment or media handling and containment protocols and procedures that must be followed within a Colo facility.

4. The CSP may have ***partial responsibility (or partial control inheritability)*** to ensure the tenant is informed of their shared responsibility for security and availability incident response planning procedures.

5. The CSP may have ***partial responsibility (or partial control inheritability)*** for cloud stack technologies within the tenant's cloud-hosted environment that the tenant has no visibility of or are only managed or accessed by the CSP's users.

6. The CSP may have ***partial responsibility (or partial control inheritability)*** to ensure the tenant is informed of, has input on, and/or provides implicit or explicit agreement with multi-party contractual arrangements that have material impact on the tenant's control requirements.

7. The CSP may have ***partial responsibility (or partial control inheritability)*** and be subject to reliance upon contractually binding service level expectations and obligations for supplying any of the following service capabilities:

   a) The tenant is permitted and granted the ability to establish external interconnections and/or implement API connections to other externally hosted on/off-prem systems.

   b) The tenant is permitted and granted the ability to control administration, native or federated provisioning of, authentication to, and the monitoring and auditing of the tenant's privileged and non-privileged physical or logical access system and user accounts.

   c) The tenant is permitted and granted the ability to establish high service availability zoning.

   d) The tenant is permitted and granted the ability to independently develop, deploy, operate, manage, monitor the lifecycle and use of the subset of discrete technology elements within the tenant's cloud instance, i.e., virtual media, endpoints or workstations, applications and their workloads, software programming, database and storage capabilities, systems and network administration functions, and the use of hardware or software (virtual) infrastructure servers, system hosts and networking components.

8. The CSP may have ***partial responsibility (or partial control inheritability)*** so as to not inhibit data privacy regulatory compliance or is subject to reliance upon contractually-binding data processor obligations in a business-to-business (B2B) relationship by the tenant as the data controller as it pertains to data subject rights for disclosure, use, individual access or third party transfers and measures involving data quality or protection.