HITRUST CSF v9.3 Release Overview and Shared Responsibility Program

November 5, 2019
CSF Version 9.3 Release
Overview
Introductory Speaker

Sarah Phillips
Senior Manager of Standards
HITRUST
Introductory Topics

- Overview of HITRUST CSF version 9.3
- Preview of what to expect for version 10.0
# Version 9.3 Authoritative Source Changes

<table>
<thead>
<tr>
<th>NEW Authoritative Sources:</th>
<th>UPDATED Authoritative Sources:</th>
</tr>
</thead>
<tbody>
<tr>
<td>California Consumer Privacy Act (CCPA)</td>
<td>AICPA TSP 100 2017 Trust Services Criteria</td>
</tr>
<tr>
<td>South Carolina Insurance Data Security Act 2018 (SCIDSA)</td>
<td>CIS CSC v7.1</td>
</tr>
<tr>
<td>NIST SP 800-171 r2</td>
<td>CMS ARS v3.1</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IRS Publication 1075 2016</td>
</tr>
<tr>
<td></td>
<td>ISO 27799:2016</td>
</tr>
<tr>
<td></td>
<td>NIST Cybersecurity Framework v1.1</td>
</tr>
</tbody>
</table>

**Did you know?**

Version 9.3 Maps to 44 Authoritative Sources
Version 9.3 Enhancements

1. Updates to the glossary to better clarify terms found in the HITRUST CSF

2. Adjusted authoritative source mappings to more fully harmonize requirements across industries and sectors

3. Adjusted selected risk and regulatory factors to ensure that only controls appropriate to a given assessment are included, streamlining the required questions
Version 10.0 Sneak Peek

1. Access to the glossary from within the platform
2. Tool Tips
3. Access to original text of mapped Authoritative Sources
4. Support for the Shared Responsibility Program
5. Enhancement to the factors, to reduce the need for ‘not applicable’ responses
6. Additional training courses and content to support organizations across the full spectrum of program maturity
Let Us Know Your Thoughts

We are building version 10 for you!

Send us your feedback:
info@hitrustalliance.net
Shared Responsibility Program

Streamlining Security Control Ownership & Responsibility with Cloud Service Providers
Today’s speakers

Becky Swain
Director, Standards Development
HITRUST

David Houlding
Principal Healthcare Lead
Microsoft

Kurt Hagerman
CxO Advisor, Cyber Strategy
Coalfire
Topics

Fireside Chat – An Industry Perspective on Shared Responsibility in the Cloud

HITRUST Shared Responsibility Program – Overview

- Program Objectives & Roadmap
- Shared Responsibility Working Group
- Shared Responsibility Model & Matrix

Closed Peer Review – What to Expect

Q&A
Fireside Chat – An Industry Perspective on Shared Responsibility in the Cloud

David Houlding, Microsoft Azure:
Why is Shared Responsibility important to Microsoft and what approach is taken to ensure Azure customers’ security and privacy assurance needs continue to be met “in the Cloud”?
Secure, Private, & Compliant Health in the Cloud

David Houlding
Principal Healthcare Lead | Industry Experiences | Cloud + AI | Azure
Microsoft
Microsoft’s approach

Privacy partnership

Secure platform

Simplifying compliance
# Security and Compliance Offerings

## Global
- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2014
- ISO 22301:2012
- ISO 9001:2015
- ISO 20000-1:2011
- CIS Benchmark
- CSA STAR Certification
- CSA STAR Attestation
- CSA STAR Self-Assessment
- WCAG 2.0 (ISO 40500:2012)

## U.S. Government
- FedRAMP High
- FedRAMP Moderate
- EAR
- DoD DISA SRG Level 5
- DoD DISA SRG Level 4
- DoD DISA SRG Level 2
- DFARS
- DoE 10 CFR Part 810
- NIST SP 800-171
- NIST CSF
- Section 508 VPATs
- FIPS 140-2
- ITAR
- CIJS
- IRS 1075

## Industry
- PCI DSS Level 1
- GLBA (US)
- FFIEC (US)
- Shared Assessments (US)
- FISC (JP)
- APRA (AU)
- OSFI (CA)
- FCA + PRA (UK)
- MAS + ABS (SG)
- FINMA (CH)
- FSA (DK)
- RBI + IRDAI (IN)
- AFM + DNB (NL)
- NBB + FSMA (BE)
- European Banking Authority
- 23 NYCRR 500 (US)
- SEC 17a-4 (US)
- CFTC 1.31 (US)
- FINRA 4511 (US)
- SOX (US)
- HIPAA BAA (US)
- HITRUST (US)
- 21 CFR Part 11 (GxP)
- MARS-E (US)
- NHS IG Toolkit (UK)
- NEN 7510:2011 (NL)
- FERPA (US)
- CDSA
- MPAA (US)
- DPP (UK)
- FACT (UK)

## Regional
- Argentina PDPA
- Australia IRAP Unclassified
- Australia IRAP Protected
- Canada Privacy Laws
- China GB 18030:2005
- China DICP (MLPS) Level 3
- China TRUCS / CCCPFF
- EN 301 549
- EU ENISA IAF
- EU Model Clauses
- EU – US Privacy Shield
- GDPR
- Germany C5
- Germany IT-Grundschutz
- India MeitY
- Japan CS Mark Gold
- Japan My Number Act
- Netherlands BIR 2012
- New Zealand Gov CIO Fwk
- Singapore MTCS Level 3
- Spain ENS
- Spain DPA
- UK Cyber Essentials Plus
- UK G-Cloud
- UK PASF
Shared responsibility, end-to-end

Customer management of risk
Data Classification and data accountability

Shared management of risk
Identity & access management | End point devices

Cloud provider management of risk
Physical | Networking

Responsibility
Data classification and accountability
Client & end-point protection
Identity & access management
Application level controls
Network controls
Host Infrastructure
Physical Security

Cloud Customer
Cloud Provider
Fireside Chat – An Industry Perspective on Shared Responsibility in the Cloud

David Houlding, Microsoft Azure:

What is Microsoft’s view of why there still remains the need for an industry-accepted solution for Shared Responsibility?
Contact

David Houlding MSc CISSP CIPP
Principal Healthcare Lead | Industry Experiences
Cloud + AI | Microsoft Corporation

✉️ David.Houlding@Microsoft.com
LinkedIn.com/in/DavidHoulding
@DavidHoulding
Kurt Hagerman, Coalfire:

From a CISO’s perspective as a buyer of cloud services and deploying applications hosted “in the Cloud,” what have you observed as the primary roadblocks that should be overcome when organizations make risk-informed decisions sharing controls with their cloud providers? … And then what about from the HITRUST assessor’s perspective?
The Case for Standardization for Shared Responsibility across CSPs

Kurt Hagerman
CxO Advisor, Cyber Strategy
Coalfire

November 2019
• Not all CSPs are created equal – your mileage will vary

• The difficulty in comparing CSPs using their own documentation

• How a standardized approach can make life easier for both CSPs and their customers (and their HITRUST assessors too)
Shared Responsibility – An Assessor’s Perspective

- Currently difficult to understand clear lines of responsibility from just the certification report

- Difficult to determine and support inheritance of controls

- A standardized approach for CSP’s to express their responsibilities will provide for better and more consistent assessments and alleviate the current challenges
Contact

Kurt Hagerman, CISSP, CISA
CxO Advisor, Cyber Strategy
Coalfire

✉️ Kurt.Hagerman@coalfire.com
LinkedIn.com/in/kurthagermanciso/
Conclusion: Why the need for an industry-acceptable solution for Shared Responsibility in the Cloud?

- We lack a common language to have a productive dialogue around cloud supply chain risk
- We are stuck with a barrier to easily come to agreement on how to parse out control responsibility
- The blurred lines of control responsibility impedes our confidence that control inheritance doesn’t result in something falling through the cracks
Becky Swain
Director, Standards Development
HITRUST

HITRUST SHARED RESPONSIBILITY PROGRAM
HITRUST Shared Responsibility Program

Strategic business initiative to address the following:

✓ To ensure cloud service providers can communicate appropriate security and privacy assurances relating to the controls associated with the services a customer has contracted

✓ To supply better guidance on the delineation of control ownership, including clarifying the more nuanced partially-shared controls that organizations rely upon

✓ To simplify the process of a cloud customers' own assurance processes by enabling and streamlining control inheritance while promoting full awareness and managed risk
Program Objectives

**HITRUST CSF®**
Shareable or inheritable controls that are supported for HITRUST CSF® v9.x to distinguish control ownership and delineate responsibility between cloud service providers and their tenants, also serving as input on the design of HITRUST CSF® v10.

**HITRUST MyCSF® Assessment Automation**
A new cloud assessment process with enhanced MyCSF control inheritance features and functionality to ensure the HITRUST CSF Certification model is designed as ‘fit-for-purpose’ for cloud service providers and their tenants.

**HITRUST Shared Responsibility Matrix**
A standard matrix template that can be customized by any SaaS, PaaS, IaaS or Colo cloud service provider to inform their tenants of which HITRUST CSF® v9.x controls are shareable or inheritable.

**HITRUST Shared Assurance® Program**
A new cloud assessment assurance methodology for testing and scoring HITRUST CSF® control requirements supported by more granular technology scoping parameters.
Shared Responsibility Working Group (WG)

Working Group Member Profile

Cloud Service Providers
External Auditors
Chief Information Security Officers
Chief Information Officers
Chief Privacy Officers
Chief Procurement Officers
Enterprise Risk Managers

Professionals in:
Supply Chain Management
Internal Audit
Third Party Risk
Our Program Roadmap Journey

Q1 2019

Q2 2019

Q3 2019

Q4 2019

Q1 2020

Q2 2020

Q3 2020

Q4 2020

SR Model & Matrix Development (Working Group)

SR Model & Matrix Beta Release

Closed Peer Review (WG)

MyCSF Cloud Assessment Build-Out & Pilots

SR Model & Matrix GA Release

MyCSF Cloud Assessment Go-Live
HITRUST Shared Responsibility Matrix

01. It is based on an industry-accepted model with a standard set of core principles and common terminology, which clarifies how compliance is shared for all cloud service model types (e.g., SaaS, PaaS, IaaS, and Colo).

02. It helps organizations navigate and more readily come to an agreement with their cloud service providers with significant clarity of multi-dimensional shared or delineated control requirement responsibility.

03. It supports an Assess Once, Inherit Many™ approach to ease the cloud assurance burden on tenants for their cloud-based workloads without introducing undue levels of risk.

04. It will serve as the basis to further enhance the MyCSF control inheritance features and functionality and support full integration with HITRUST CSF v10.
### HITRUST Shared Responsibility Model

#### Not Shared

<table>
<thead>
<tr>
<th>No Outsourced Control Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Tenant has no reliance upon outsourced technology services/capabilities</td>
</tr>
<tr>
<td>• Tenant's system components and/or facilities not shared with CSP</td>
</tr>
<tr>
<td>• CSP’s control design and/or continual operating effectiveness (or lack thereof) has no material impact on tenant</td>
</tr>
</tbody>
</table>

#### Shared

<table>
<thead>
<tr>
<th>Outsourced Control Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Fully Inheritable</strong> – Tenant &amp; CSP share common system components and/or facilities but tenant is not involved in control design and/or continual operating effectiveness</td>
</tr>
<tr>
<td>• <strong>Joint Reliance</strong> – Tenant &amp; CSP share common system components and/or facilities and both parties are equally responsible for control design and/or continual operating effectiveness</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Control Requirement Reliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• <strong>Control Enablement</strong> – Tenant relies upon use of outsourced technology services/capabilities</td>
</tr>
<tr>
<td>• <strong>Control Collaboration</strong> – Tenant relies upon performing activity dictated by CSP</td>
</tr>
<tr>
<td>• <strong>Control Relay</strong> – Tenant relies upon input from CSP</td>
</tr>
</tbody>
</table>
Closed Peer Review – What to Expect

Kickoff meeting: Wed, Dec 5th @ 12pm CT (Save the date!)

Review period: Dec 6th to Jan 15th

Participation: Open only to Shared Responsibility (SR) Working Group members

Objectives for industry feedback:

a) Design review of HITRUST Shared Responsibility Matrix beta release to confirm market feasibility as “fit-for-purpose” to prep for Q1 2020 GA release

b) Input on MyCSF Cloud Assessment approach and preliminary operational & technical design concepts

CALL TO ACTION ➔ Sign-up to join the SR Working Group by Thursday, Nov 21st

Go to: https://hitrustalliance.net/hitrust-shared-responsibility-program
Questions?
For more information on HITRUST’s Programs visit www.HITRUSTAlliance.net

To view our latest documents, visit the Content Spotlight