HITRUST 2022 COLLABORATE

How to Utilize MyCSF Inheritance with HITRUST Shared Responsibility Matrices (SRMs)

Agenda

- Overview:
    - About the HITRUST Shared Responsibility and Inheritance Program
    - HITRUST Customer Qualifications

- Utilizing MyCSF Inheritance with HITRUST Shared Responsibility Matrices (SRMs)…
    - As the Inheritance Provider
    - As the Assessed Entity (or External Assessor)

Overview

The HITRUST Shared Responsibility and Inheritance Program

DID YOU KNOW?

For an r2 Validated Assessment, your organization can inherit up to **60%** of controls from cloud service providers!

For an i1 Validated Assessment, your organization can inherit up to **80%** of controls from cloud service providers!

Adding Inheritance Efficiency Saves Time, Effort, and Cost on HITRUST Assessments!

External Inheritance

Organizations can use their MyCSF® subscription to import control assessment results and scores from their other HITRUST Validated Assessments that have been published (enabled) for External Inheritance by hosting, cloud, or other service providers.

Internal Inheritance

Organizations can use their MyCSF® subscription to leverage and repurpose controls assessment results and scores that are internally inheritable to or from their other current or previous HITRUST Assessments.

INHERITANCE PROVIDER
HITRUST®
r2 CERTIFIED

INHERITANCE PROVIDER
HITRUST®
i1 CERTIFIED

Key Inheritance Benefits

Reduces the need for duplicative and redundant direct controls testing that is covered and obtained under a prior valid assessment.

Identifies control mappings and leverages assessment results within one system to efficiently process Inheritance information exchange.

Provides the transparency and visibility needed to fully understand and effectively inherit existing controls assessment data.

The industry's only Inheritance capability for third-party assurances, especially well-suited for shared cloud-based control environments.

Utilizing MyCSF Inheritance with HITRUST Shared Responsibility Matrices (SRMs)

Some Key Terms We Will Use:

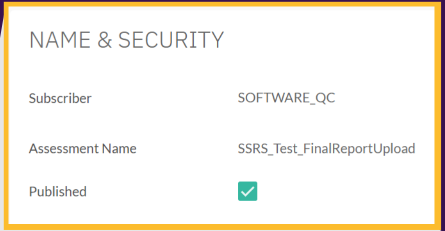
Term	Definition
Inheritance	The sharing of HITRUST Assessment results between HITRUST Assessment(s) through purposeful electronic workflows, typically in the context of shared responsibility in the performance of cybersecurity controls
Internal Inheritance	Using inheritance to share assessment results between assessments of a single organization (e.g., between a shared IT service and the business)
External Inheritance	Using inheritance to share assessment results between assessments of different organizations (e.g., between a CSP and its tenants)
Inheritance Provider	An organization who has published / enabled their HITRUST assessment for external inheritance
MyCSF	HITRUST's assessment platform
SRM	Shared Responsibility Matrix, the (currently Excel-based) mechanism by which security obligations of a provider (typically CSPs) and its users are communicated, to ensure accountability
Inheritability Values	Information describing whether a requirement is fully, partially, or not inheritable (and why)

HITRUST Customer Qualifications: Inheritance Provider

Type	Description
MyCSF Subscription	INTERNAL & EXTERNAL INHERITANCE: Assessment owner is an active annual MyCSF subscriber with a Corporate or Premier-level subscription.
CSF Assurance Requirements	EXTERNAL INHERITANCE (ONLY): • The assessment object within MyCSF is in a ‘Completed’ state with the final report date posted and remaining effective during its lifespan for the following supported assessment types: ✓ r2 Validated—for a period of 2 years after the final report date and timely completion of the interim assessment by the 1-year anniversary date of final report date. ✓ i1 Validated—for a period of 1 year after the final report date. • The assessment object is configured to be ‘Published’ (enabled) for external inheritance with the box checked on the “Name & Security” page within MyCSF and inheritance requests are processed in a reasonably timely manner (including consenting to terms/conditions for inheritance-related sharing/exchange of privileged customer information).
Additional Benefits	Inheritance Providers are eligible to have a HITRUST Shared Responsibility Matrix (SRM) published that is tailored to their inheritable assessment and access to a press kit that includes the promotional material and guidelines (e.g., logo and press release template).

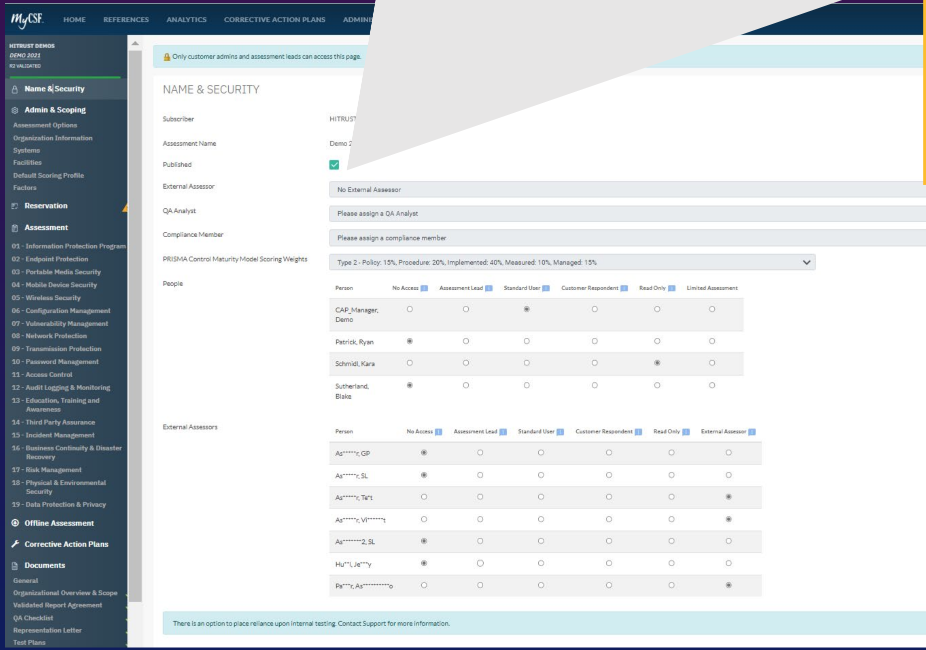
External **Inheritance** – Publishing (Enabling) **by Inheritance Provider**

- ‘Published’ box checked on “Name & Security” page within assessment object



NAME & SECURITY

Subscriber	SOFTWARE_QC
Assessment Name	SSRS_Test_FinalReportUpload
Published	☑



HITRUST DEMOS
DEMO 2021
R2 VALIDATED

- Name & Security
- Admin & Scoping
  - Assessment Options
  - Organization Information
  - Systems
  - Facilities
  - Default Scoring Profile
  - Factors
- Reservation
- Assessment
  - 01 - Information Protection Program
  - 02 - Endpoint Protection
  - 03 - Portable Media Security
  - 04 - Mobile Device Security
  - 05 - Wireless Security
  - 06 - Configuration Management
  - 07 - Vulnerability Management
  - 08 - Network Protection
  - 09 - Transmission Protection
  - 10 - Password Management
  - 11 - Access Control
  - 12 - Audit Logging & Monitoring
  - 13 - Education, Training and Awareness
  - 14 - Third Party Assurance
  - 15 - Incident Management
  - 16 - Business Continuity & Disaster Recovery
  - 17 - Risk Management
  - 18 - Physical & Environmental Security
  - 19 - Data Protection & Privacy
- Offline Assessment
- Corrective Action Plans
- Documents
  - General
  - Organizational Overview & Scope
  - Validated Report Agreement
  - QA Checklist
  - Representation Letter
  - Test Plans

Only customer admins and assessment leads can access this page.

NAME & SECURITY

Subscriber	HITRUST
Assessment Name	Demo 2
Published	☑
External Assessor	No External Assessor
QA Analyst	Please assign a QA Analyst
Compliance Member	Please assign a compliance member
PRISMA Control Maturity Model Scoring Weights	Type 2 - Policy: 15%, Procedure: 20%, Implemented: 40%, Measured: 10%, Managed: 15%

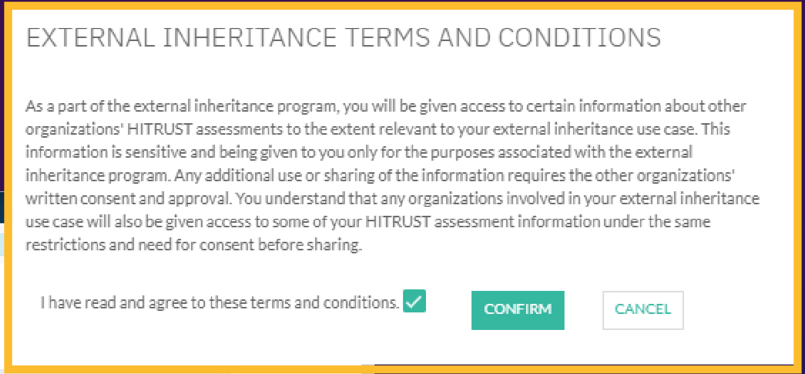
People

Person	No Access	Assessment Lead	Standard User	Customer Respondent	Read Only	Limited Assessment
CAP_Manager, Demo	○	○	●	○	○	○
Patrick, Ryan	●	○	○	○	○	○
Schmidl, Kara	○	○	○	○	●	○
Sutherland, Blake	●	○	○	○	○	○

External Assessors

Person	No Access	Assessment Lead	Standard User	Customer Respondent	Read Only	External Assessor
As*****r, GP	●	○	○	○	○	○
As*****r, SL	●	○	○	○	○	○
As*****r, Te*t	○	○	○	○	○	●
As*****r, Vi******t	○	○	○	○	○	●
As*******2, SL	●	○	○	○	○	○
Hu**l, Je***y	●	○	○	○	○	○
Pa***r, As**********o	○	○	○	○	○	●

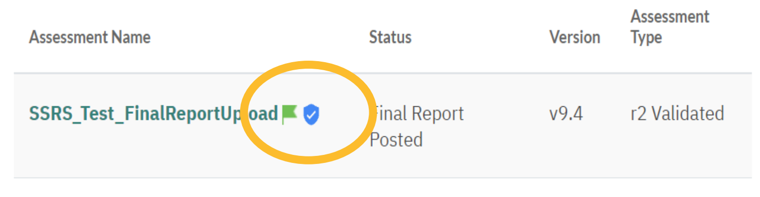
There is an option to place reliance upon internal testing. Contact Support for more information.



EXTERNAL INHERITANCE TERMS AND CONDITIONS

As a part of the external inheritance program, you will be given access to certain information about other organizations' HITRUST assessments to the extent relevant to your external inheritance use case. This information is sensitive and being given to you only for the purposes associated with the external inheritance program. Any additional use or sharing of the information requires the other organizations' written consent and approval. You understand that any organizations involved in your external inheritance use case will also be given access to some of your HITRUST assessment information under the same restrictions and need for consent before sharing.

I have read and agree to these terms and conditions. ☑



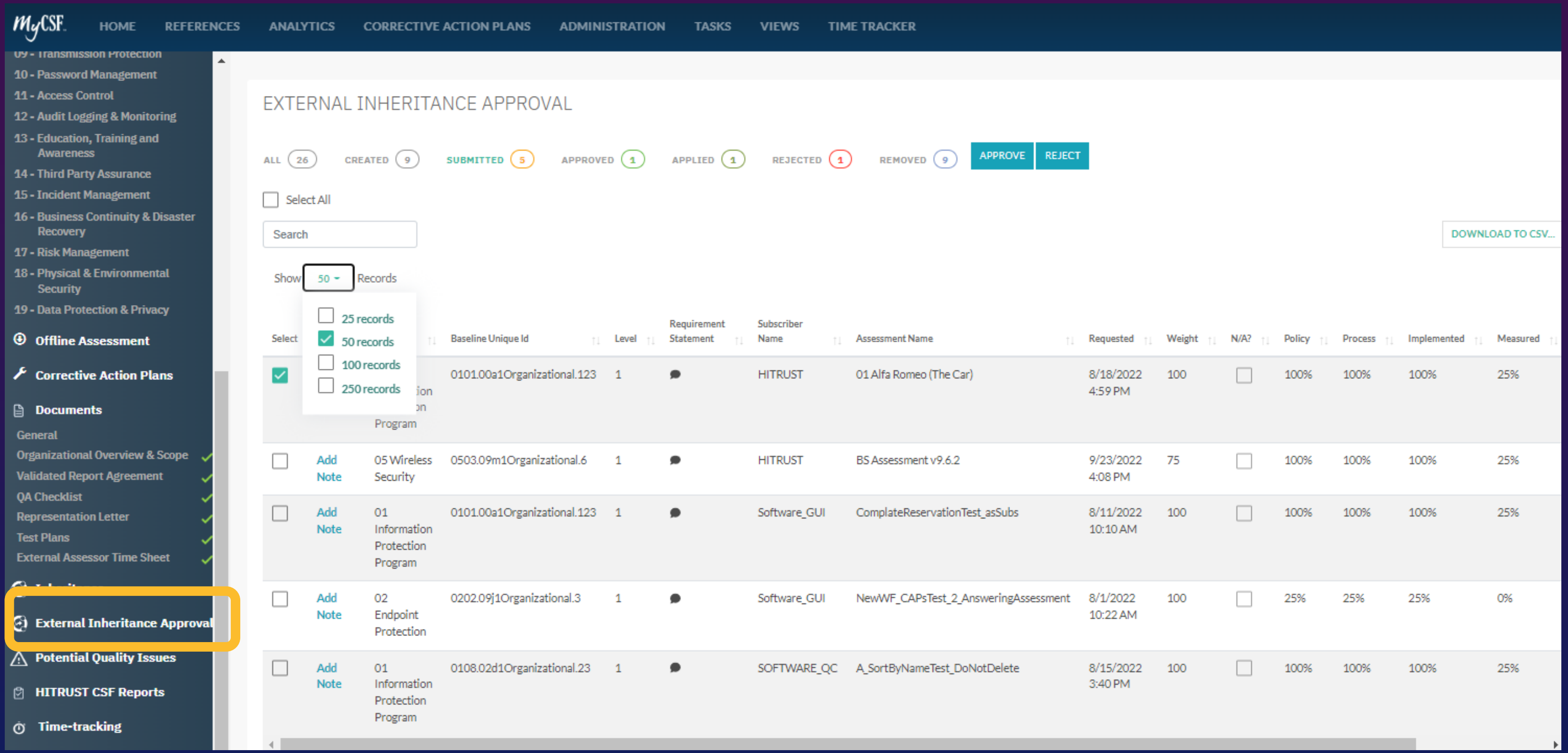
Assessment Name	Status	Version	Assessment Type
SSRS_Test_FinalReportUpload	Final Report Posted	v9.4	r2 Validated

- New badge on Inheritance Provider’s home page shows that an assessment object is published/enabled for external inheritance (MyCSF Release 1.16)

HITRUST 2022 COLLABORATE

External **Inheritance** – Inheritance Table **for Inheritance Provider**

- Inheritance approval table contains consolidated view of all inheriting customers
  - Allows for bulk processing of submitted inheritance requests
  - New enhancements includes ‘ALL’ count and improved data filtering functionality (MyCSF Release 1.16)
  - Future Inheritance 2.0 enhancements to include single-click navigation from toolbar menu and data field updates consistent with assessment-level inheritance table data field updates



EXTERNAL INHERITANCE APPROVAL

ALL 26 CREATED 9 SUBMITTED 5 APPROVED 1 APPLIED 1 REJECTED 1 REMOVED 9

□ Select All

Search

Show 50 Records

□ 25 records
☑ 50 records
□ 100 records
□ 250 records

Select			Baseline Unique Id	Level	Requirement Statement	Subscriber Name	Assessment Name	Requested	Weight	N/A?	Policy	Process	Implemented	Measured
☑		ion on Program	0101.00a1Organizational.123	1	●	HITRUST	01 Alfa Romeo (The Car)	8/18/2022 4:59 PM	100	□	100%	100%	100%	25%
□	Add Note	05 Wireless Security	0503.09m1Organizational.6	1	●	HITRUST	BS Assessment v9.6.2	9/23/2022 4:08 PM	75	□	100%	100%	100%	25%
□	Add Note	01 Information Protection Program	0101.00a1Organizational.123	1	●	Software_GUI	ComplateReservationTest_asSubs	8/11/2022 10:10 AM	100	□	100%	100%	100%	25%
□	Add Note	02 Endpoint Protection	0202.09j1Organizational.3	1	●	Software_GUI	NewWF_CAPsTest_2_AnsweringAssessment	8/1/2022 10:22 AM	100	□	25%	25%	25%	0%
□	Add Note	01 Information Protection Program	0108.02d1Organizational.23	1	●	SOFTWARE_QC	A_SortByNameTest_DoNotDelete	8/15/2022 3:40 PM	100	□	100%	100%	100%	25%

HITRUST Shared Responsibility Matrices (SRMs)

Optimal Managed Risk Solutions for Sharing Information Security Control Assurances

Reduces Time, Effort, and Cost by Inheriting Control Scoring, Assessment Information, and Results

HITRUST Shared Responsibility Matrix
No-cost, easy-to-use, out-of-box, baseline template with pre-populated shared responsibility and controls inheritability that are perfectly suited for shared cloud environments.

HITRUST Shared Responsibility Matrices are a Comprehensive Blueprint to Identify Shared Controls and Facilitate Sharing

HITRUST

Aptible

aws

cloudticity

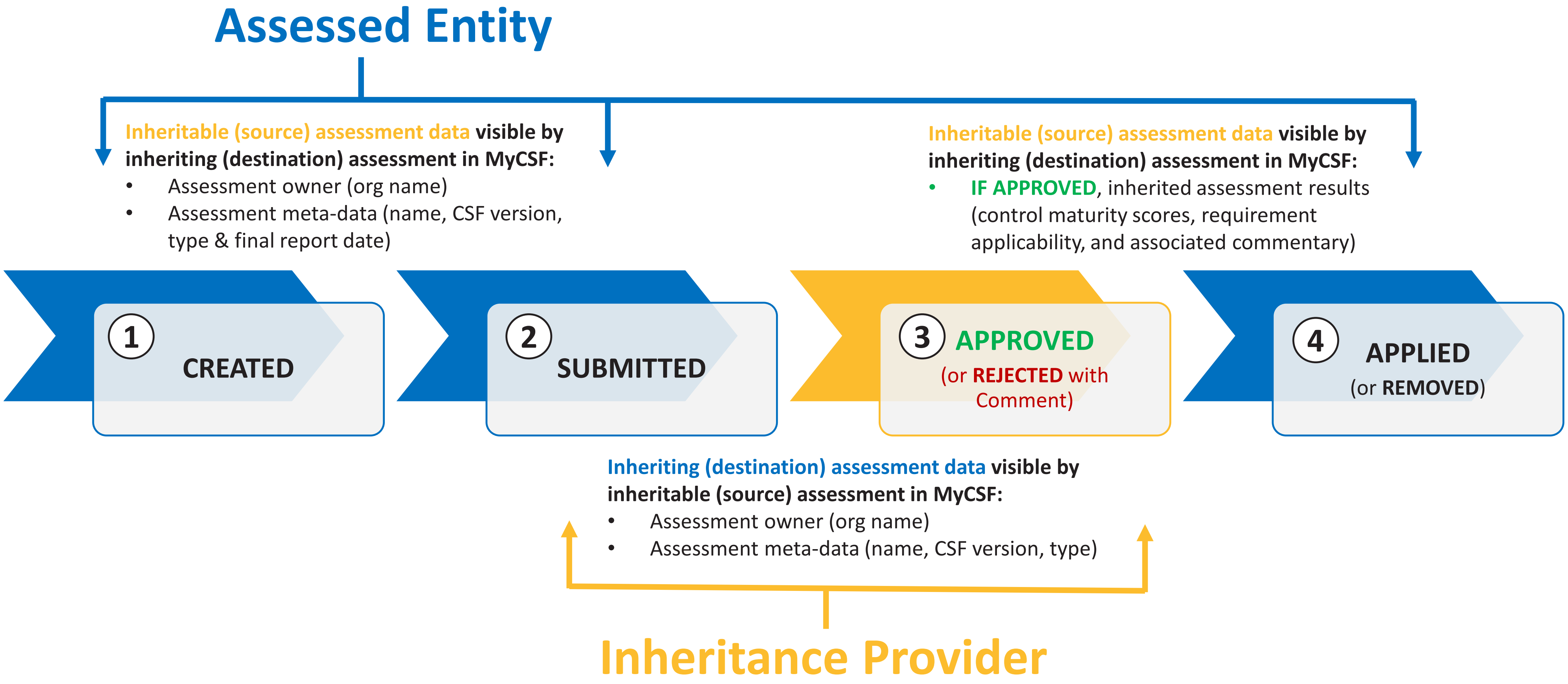
Google

Microsoft Azure

ORACLE Cloud Infrastructure

snowflake

External Inheritance – Workflow Process Flow & Data



Assessed Entity

Inheritable (source) assessment data visible by inheriting (destination) assessment in MyCSF:

- Assessment owner (org name)
- Assessment meta-data (name, CSF version, type & final report date)

Inheritable (source) assessment data visible by inheriting (destination) assessment in MyCSF:

- **IF APPROVED**, inherited assessment results (control maturity scores, requirement applicability, and associated commentary)

1 **CREATED**

2 **SUBMITTED**

3 **APPROVED** (or **REJECTED** with Comment)

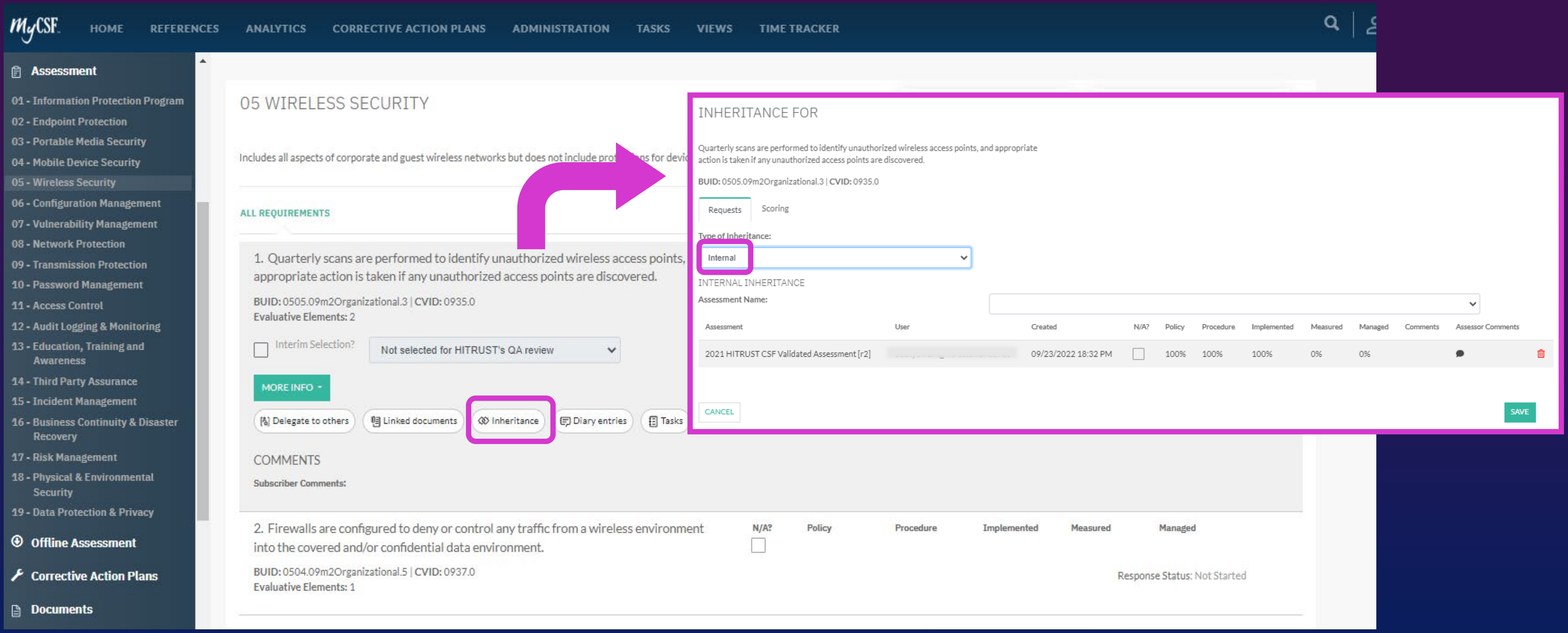
4 **APPLIED** (or **REMOVED**)

Inheriting (destination) assessment data visible by inheritable (source) assessment in MyCSF:

- Assessment owner (org name)
- Assessment meta-data (name, CSF version, type)

Inheritance Provider

Internal **Inheritance** – Initiating in Assessment Object (via Inheritance Model) **by Assessed Entity**



MyCSF
HOME
REFERENCES
ANALYTICS
CORRECTIVE ACTION PLANS
ADMINISTRATION
TASKS
VIEWS
TIME TRACKER
Assessment
01 - Information Protection Program
02 - Endpoint Protection
03 - Portable Media Security
04 - Mobile Device Security
05 - Wireless Security
06 - Configuration Management
07 - Vulnerability Management
08 - Network Protection
09 - Transmission Protection
10 - Password Management
11 - Access Control
12 - Audit Logging & Monitoring
13 - Education, Training and Awareness
14 - Third Party Assurance
15 - Incident Management
16 - Business Continuity & Disaster Recovery
17 - Risk Management
18 - Physical & Environmental Security
19 - Data Protection & Privacy
Offline Assessment
Corrective Action Plans
Documents
MORE INFO
Delegate to others
Linked documents
Inheritance
Diary entries
Tasks

05 WIRELESS SECURITY

Includes all aspects of corporate and guest wireless networks but does not include prot... ns for devic...

ALL REQUIREMENTS

1. Quarterly scans are performed to identify unauthorized wireless access points, ... appropriate action is taken if any unauthorized access points are discovered.

BUID: 0505.09m2Organizational.3 | **CVID:** 0935.0
Evaluative Elements: 2

□ Interim Selection? Not selected for HITRUST's QA review

COMMENTS

Subscriber Comments:

2. Firewalls are configured to deny or control any traffic from a wireless environment into the covered and/or confidential data environment.

BUID: 0504.09m2Organizational.5 | **CVID:** 0937.0
Evaluative Elements: 1

N/A?	Policy	Procedure	Implemented	Measured	Managed
□					

Response Status: Not Started

INHERITANCE FOR

Quarterly scans are performed to identify unauthorized wireless access points, and appropriate action is taken if any unauthorized access points are discovered.

BUID: 0505.09m2Organizational.3 | **CVID:** 0935.0

Requests | Scoring

Type of Inheritance: Internal

INTERNAL INHERITANCE

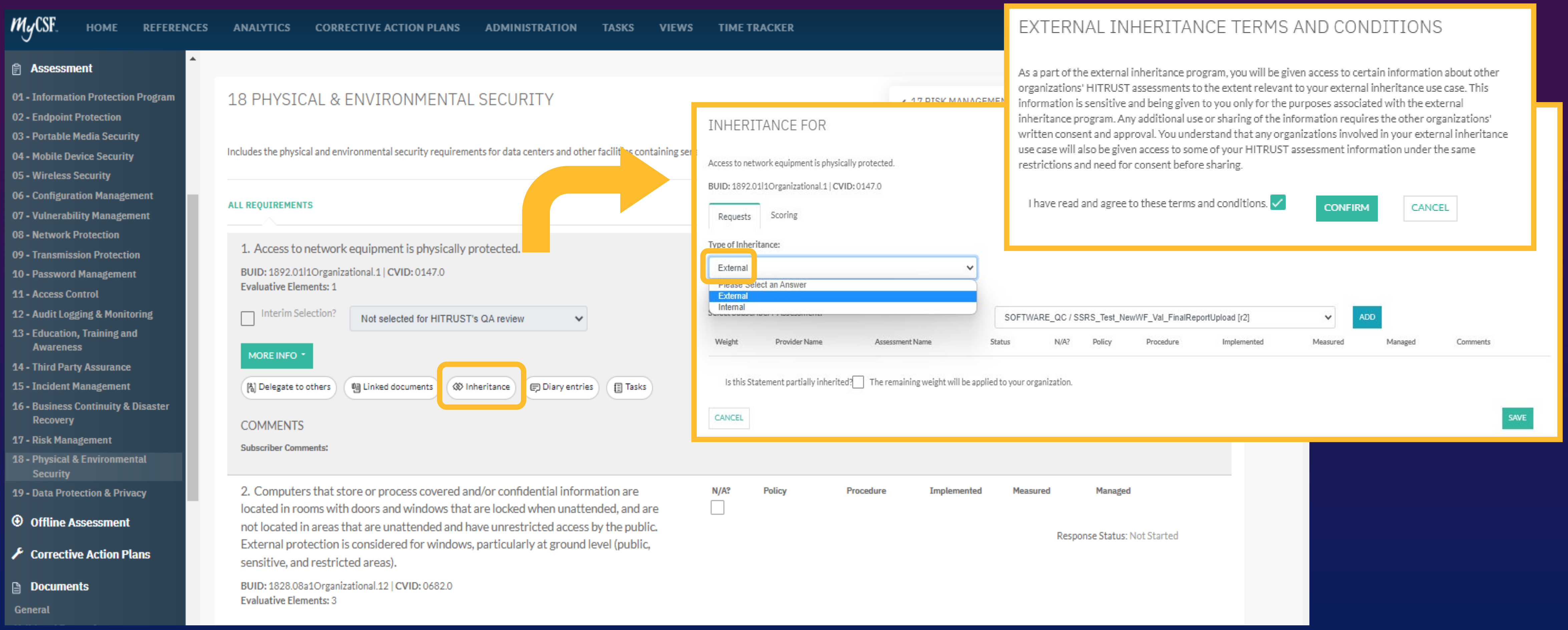
Assessment Name:

Assessment	User	Created	N/A?	Policy	Procedure	Implemented	Measured	Managed	Comments	Assessor Comments
2021 HITRUST CSF Validated Assessment [r2]	[redacted]	09/23/2022 18:32 PM	□	100%	100%	100%	0%	0%		

CANCEL SAVE

HITRUST 2022 COLLABORATE

External **Inheritance** – Initiating in Assessment Object (via Inheritance Model) **by Assessed Entity**



Assessment

- 01 - Information Protection Program
- 02 - Endpoint Protection
- 03 - Portable Media Security
- 04 - Mobile Device Security
- 05 - Wireless Security
- 06 - Configuration Management
- 07 - Vulnerability Management
- 08 - Network Protection
- 09 - Transmission Protection
- 10 - Password Management
- 11 - Access Control
- 12 - Audit Logging & Monitoring
- 13 - Education, Training and Awareness
- 14 - Third Party Assurance
- 15 - Incident Management
- 16 - Business Continuity & Disaster Recovery
- 17 - Risk Management
- 18 - Physical & Environmental Security
- 19 - Data Protection & Privacy

Offline Assessment

Corrective Action Plans

Documents

General

18 PHYSICAL & ENVIRONMENTAL SECURITY

‹ 17 RISK MANAGEMEN

Includes the physical and environmental security requirements for data centers and other facilit s containing ser

ALL REQUIREMENTS

1. Access to network equipment is physically protected.

BUID: 1892.01l1Organizational.1 | **CVID:** 0147.0
Evaluative Elements: 1

□ Interim Selection? Not selected for HITRUST's QA review

COMMENTS

Subscriber Comments:

2. Computers that store or process covered and/or confidential information are located in rooms with doors and windows that are locked when unattended, and are not located in areas that are unattended and have unrestricted access by the public. External protection is considered for windows, particularly at ground level (public, sensitive, and restricted areas).

BUID: 1828.08a1Organizational.12 | **CVID:** 0682.0
Evaluative Elements: 3

N/A?	Policy	Procedure	Implemented	Measured	Managed
□					

Response Status: Not Started

INHERITANCE FOR

Access to network equipment is physically protected.

BUID: 1892.01l1Organizational.1 | **CVID:** 0147.0

Type of Inheritance: External

SOFTWARE_QC / SSRS_Test_NewWF_Val_FinalReportUpload [r2]

Weight	Provider Name	Assessment Name	Status	N/A?	Policy	Procedure	Implemented	Measured	Managed	Comments

Is this Statement partially inherited? □ The remaining weight will be applied to your organization.

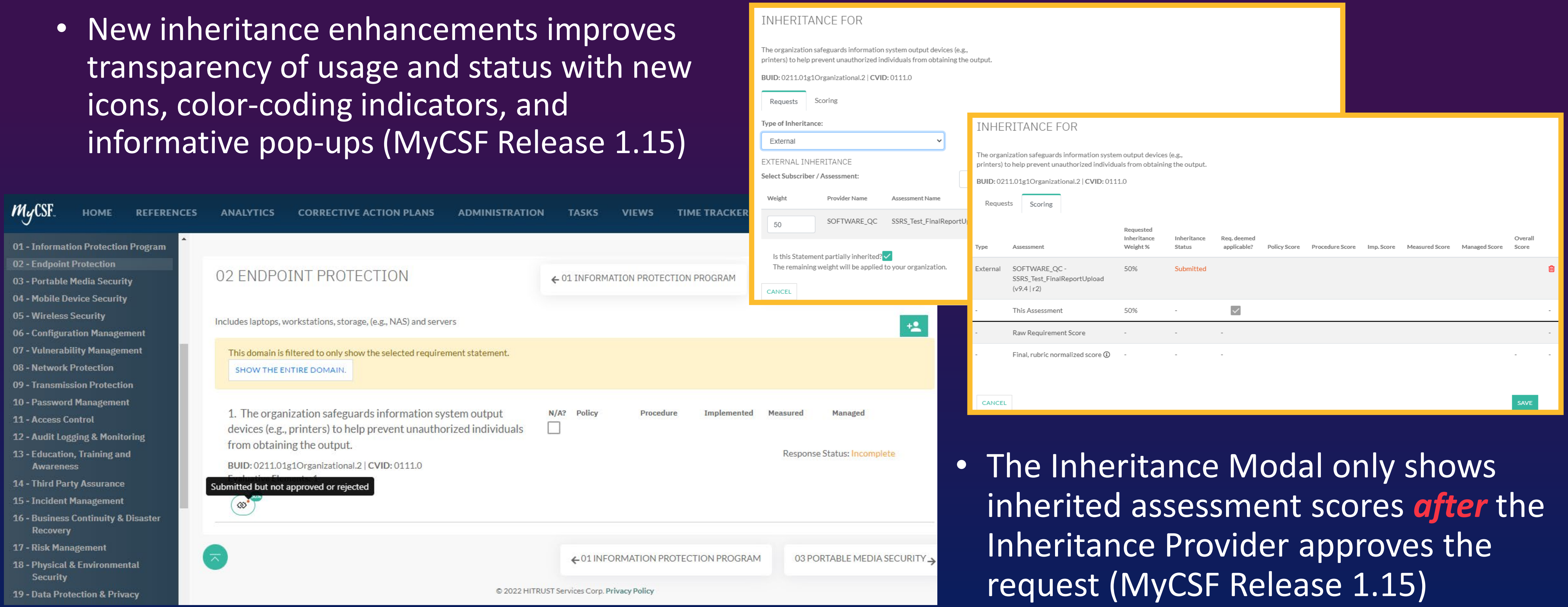
EXTERNAL INHERITANCE TERMS AND CONDITIONS

As a part of the external inheritance program, you will be given access to certain information about other organizations' HITRUST assessments to the extent relevant to your external inheritance use case. This information is sensitive and being given to you only for the purposes associated with the external inheritance program. Any additional use or sharing of the information requires the other organizations' written consent and approval. You understand that any organizations involved in your external inheritance use case will also be given access to some of your HITRUST assessment information under the same restrictions and need for consent before sharing.

I have read and agree to these terms and conditions. ☑

External **Inheritance** – Inheritance Model: Requests Submitted **by Assessed Entity**

- New inheritance enhancements improves transparency of usage and status with new icons, color-coding indicators, and informative pop-ups (MyCSF Release 1.15)



01 - Information Protection Program
02 - Endpoint Protection
03 - Portable Media Security
04 - Mobile Device Security
05 - Wireless Security
06 - Configuration Management
07 - Vulnerability Management
08 - Network Protection
09 - Transmission Protection
10 - Password Management
11 - Access Control
12 - Audit Logging & Monitoring
13 - Education, Training and Awareness
14 - Third Party Assurance
15 - Incident Management
16 - Business Continuity & Disaster Recovery
17 - Risk Management
18 - Physical & Environmental Security
19 - Data Protection & Privacy

02 ENDPOINT PROTECTION

← 01 INFORMATION PROTECTION PROGRAM

Includes laptops, workstations, storage, (e.g., NAS) and servers

This domain is filtered to only show the selected requirement statement.

SHOW THE ENTIRE DOMAIN.

1. The organization safeguards information system output devices (e.g., printers) to help prevent unauthorized individuals from obtaining the output.

N/A?	Policy	Procedure	Implemented	Measured	Managed
□					

Response Status: Incomplete

BUID: 0211.01g1Organizational.2 | CVID: 0111.0

Submitted but not approved or rejected

← 01 INFORMATION PROTECTION PROGRAM

03 PORTABLE MEDIA SECURITY →

© 2022 HITRUST Services Corp. Privacy Policy

INHERITANCE FOR

The organization safeguards information system output devices (e.g., printers) to help prevent unauthorized individuals from obtaining the output.

BUID: 0211.01g1Organizational.2 | **CVID:** 0111.0

Requests | Scoring

Type of Inheritance: External

EXTERNAL INHERITANCE

Select Subscriber / Assessment:

Weight	Provider Name	Assessment Name
50	SOFTWARE_QC	SSRS_Test_FinalReportU

Is this Statement partially inherited? ☑
The remaining weight will be applied to your organization.

CANCEL

INHERITANCE FOR

The organization safeguards information system output devices (e.g., printers) to help prevent unauthorized individuals from obtaining the output.

BUID: 0211.01g1Organizational.2 | **CVID:** 0111.0

Requests | Scoring

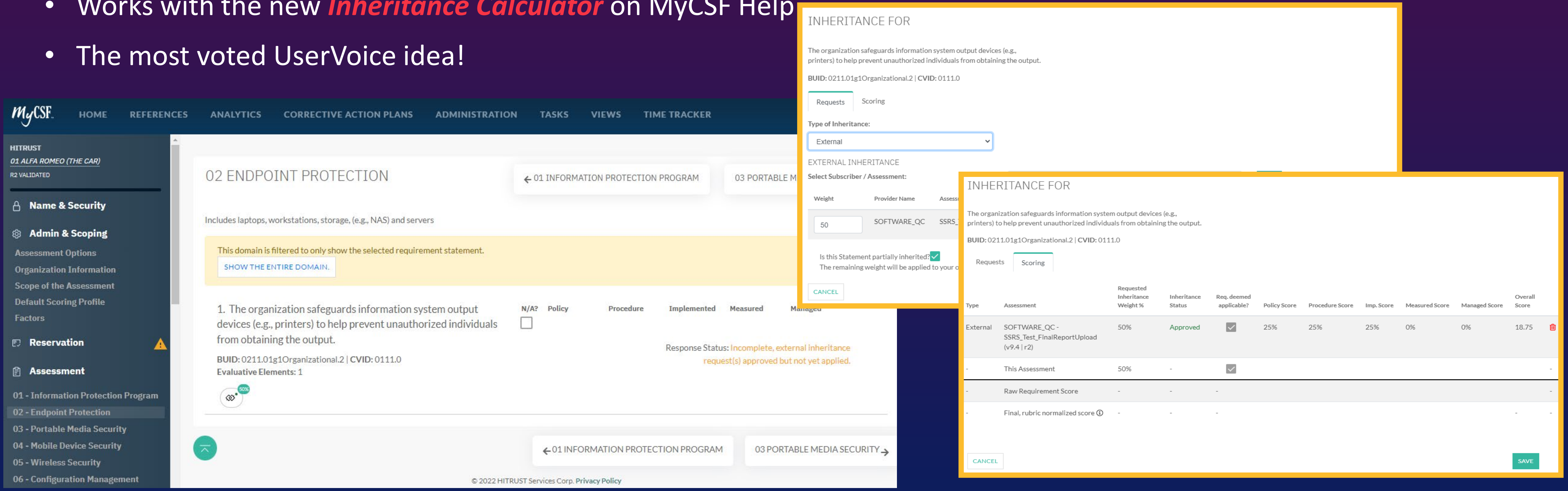
Type	Assessment	Requested Inheritance Weight %	Inheritance Status	Req. deemed applicable?	Policy Score	Procedure Score	Imp. Score	Measured Score	Managed Score	Overall Score	
External	SOFTWARE_QC - SSRS_Test_FinalReportUpload (v9.4 | r2)	50%	Submitted								
-	This Assessment	50%	-	☑							-
-	Raw Requirement Score	-	-	-							-
-	Final, rubric normalized score ⓘ	-	-	-						-	-

CANCEL SAVE

- The Inheritance Modal only shows inherited assessment scores ***after*** the Inheritance Provider approves the request (MyCSF Release 1.15)

External **Inheritance** – Inheritance Model: Requests Approved **by Inheritance Provider**

- New inheritance enhancements adds 2nd scoring tab that provides a breakdown of the complex rubric-based scoring of inherited assessment scores (MyCSF Release 1.15)
  - Works with the new ***Inheritance Calculator*** on MyCSF Help
  - The most voted UserVoice idea!



02 ENDPOINT PROTECTION

Includes laptops, workstations, storage, (e.g., NAS) and servers

This domain is filtered to only show the selected requirement statement.

1. The organization safeguards information system output devices (e.g., printers) to help prevent unauthorized individuals from obtaining the output.

N/A? □ Policy Procedure Implemented Measured Managed

BUID: 0211.01g1Organizational.2 | CVID: 0111.0
Evaluative Elements: 1

Response Status: Incomplete, external inheritance request(s) approved but not yet applied.

© 2022 HITRUST Services Corp. Privacy Policy

INHERITANCE FOR

The organization safeguards information system output devices (e.g., printers) to help prevent unauthorized individuals from obtaining the output.

BUID: 0211.01g1Organizational.2 | **CVID:** 0111.0

Type of Inheritance: External

EXTERNAL INHERITANCE

Select Subscriber / Assessment:

Weight	Provider Name	Assess
50	SOFTWARE_QC	SSRS_

Is this Statement partially inherited? ☑
The remaining weight will be applied to your o

INHERITANCE FOR

The organization safeguards information system output devices (e.g., printers) to help prevent unauthorized individuals from obtaining the output.

BUID: 0211.01g1Organizational.2 | **CVID:** 0111.0

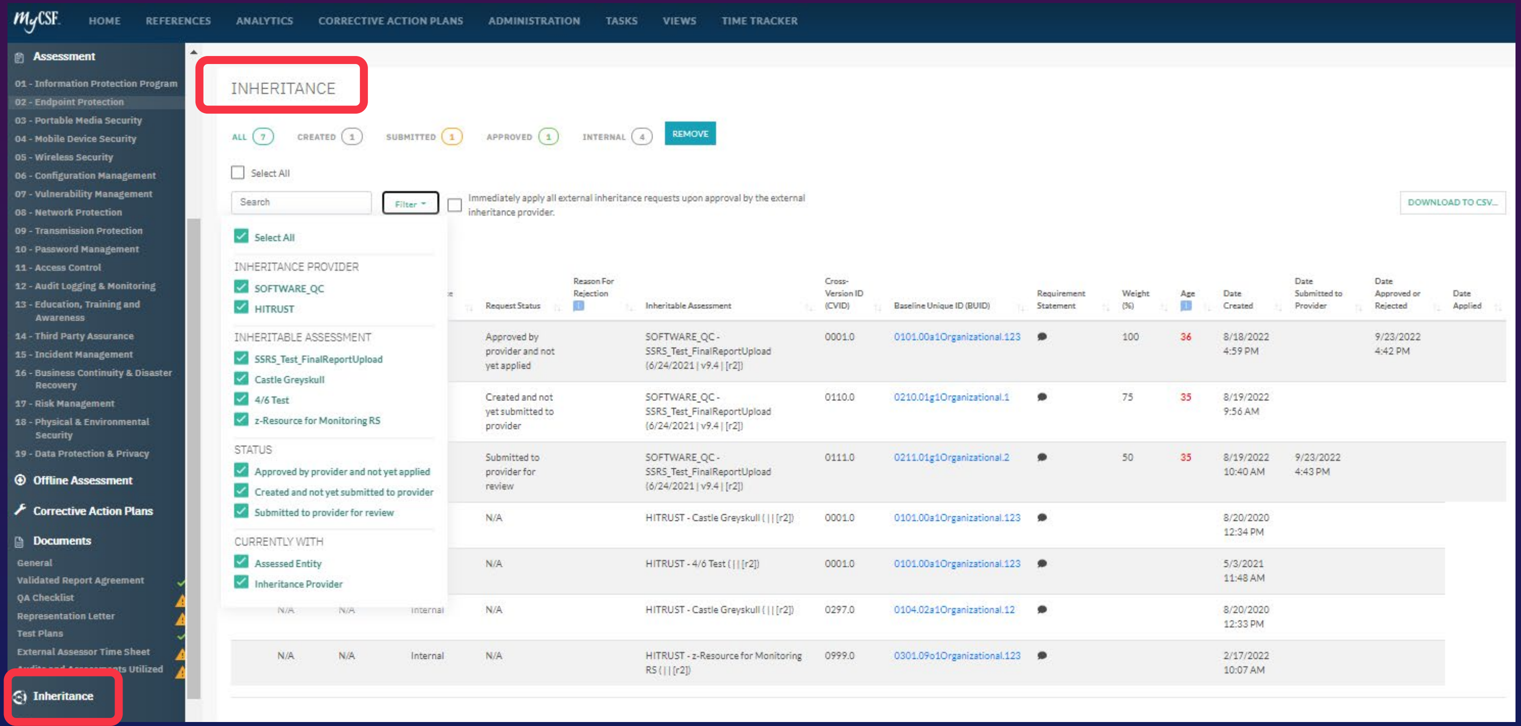
Type	Assessment	Requested Inheritance Weight %	Inheritance Status	Req. deemed applicable?	Policy Score	Procedure Score	Imp. Score	Measured Score	Managed Score	Overall Score	
External	SOFTWARE_QC - SSRS_Test_FinalReportUpload (v9.4 | r2)	50%	Approved	☑	25%	25%	25%	0%	0%	18.75	
-	This Assessment	50%	-	☑							-
-	Raw Requirement Score	-	-	-							-
-	Final, rubric normalized score ⓘ	-	-	-						-	-

HITRUST 2022 COLLABORATE

©2022 HITRUST

Internal & *External* Inheritance – Inheritance Table for the Assessed Entity

- Assessment-level Inheritance Table is used for submitting external inheritance requests (per request or in bulk) to the Inheritance Provider for processing and checking status
  - New enhancement adds ***Internal Inheritance*** support and title of page renamed (included in MyCSF Release 1.15 & 1.16)
  - New enhancement adds new data filtering functionality for improved usability (MyCSF Release 1.15)
  - New enhancement refreshes the table's data fields (i.e., CVID, request aging, etc.) for improved transparency and to align to newer functionality enhancements (MyCSF Release 1.15)


MyCSF
HOME
REFERENCES
ANALYTICS
CORRECTIVE ACTION PLANS
ADMINISTRATION
TASKS
VIEWS
TIME TRACKER
Assessment
01 - Information Protection Program
02 - Endpoint Protection
03 - Portable Media Security
04 - Mobile Device Security
05 - Wireless Security
06 - Configuration Management
07 - Vulnerability Management
08 - Network Protection
09 - Transmission Protection
10 - Password Management
11 - Access Control
12 - Audit Logging & Monitoring
13 - Education, Training and Awareness
14 - Third Party Assurance
15 - Incident Management
16 - Business Continuity & Disaster Recovery
17 - Risk Management
18 - Physical & Environmental Security
19 - Data Protection & Privacy
Offline Assessment
Corrective Action Plans
Documents
General
Validated Report Agreement
QA Checklist
Representation Letter
Test Plans
External Assessor Time Sheet
Audits and Assessments Utilized
Inheritance
REMOVE
Search
Filter
DOWNLOAD TO CSV...

INHERITANCE

ALL 7 CREATED 1 SUBMITTED 1 APPROVED 1 INTERNAL 4

□ Select All

□ Immediately apply all external inheritance requests upon approval by the external inheritance provider.

☑ Select All

INHERITANCE PROVIDER
☑ SOFTWARE_QC
☑ HITRUST

INHERITABLE ASSESSMENT
☑ SSRS_Test_FinalReportUpload
☑ Castle Greyskull
☑ 4/6 Test
☑ z-Resource for Monitoring RS

STATUS
☑ Approved by provider and not yet applied
☑ Created and not yet submitted to provider
☑ Submitted to provider for review

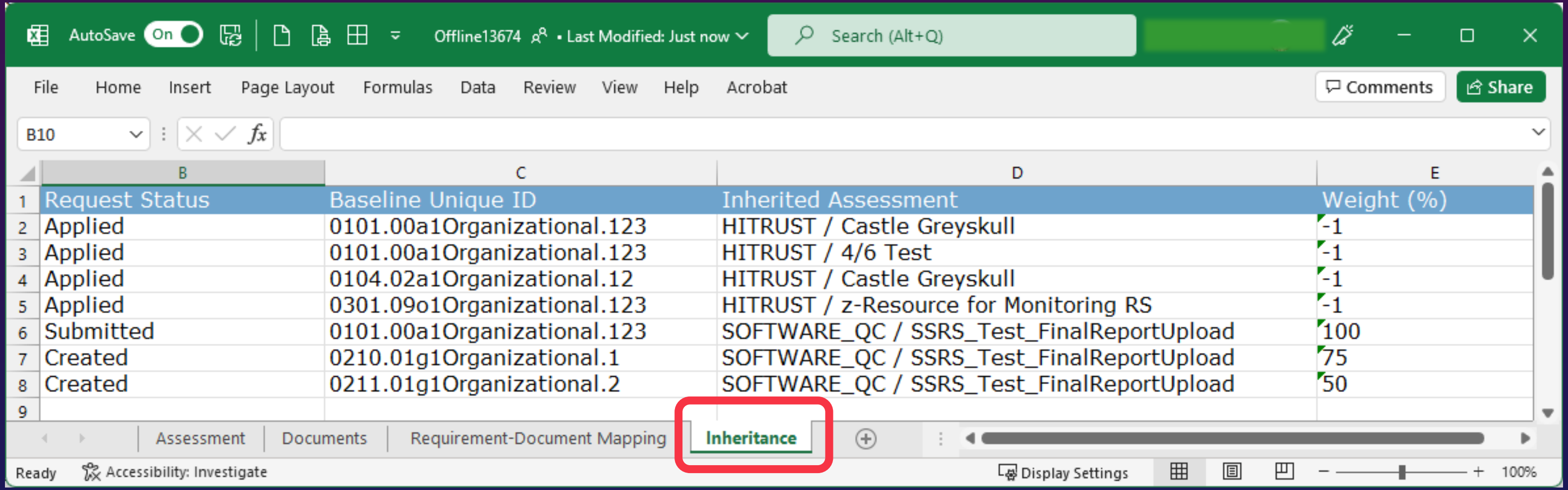
CURRENTLY WITH
☑ Assessed Entity
☑ Inheritance Provider

		e	Request Status	Reason For Rejection	Inheritable Assessment	Cross-Version ID (CVID)	Baseline Unique ID (BUID)	Requirement Statement	Weight (%)	Age	Date Created	Date Submitted to Provider	Date Approved or Rejected	Date Applied
			Approved by provider and not yet applied		SOFTWARE_QC - SSRS_Test_FinalReportUpload (6/24/2021 | v9.4 | [r2])	0001.0	0101.00a1Organizational.123	💬	100	36	8/18/2022 4:59 PM		9/23/2022 4:42 PM	
			Created and not yet submitted to provider		SOFTWARE_QC - SSRS_Test_FinalReportUpload (6/24/2021 | v9.4 | [r2])	0110.0	0210.01g1Organizational.1	💬	75	35	8/19/2022 9:56 AM			
			Submitted to provider for review		SOFTWARE_QC - SSRS_Test_FinalReportUpload (6/24/2021 | v9.4 | [r2])	0111.0	0211.01g1Organizational.2	💬	50	35	8/19/2022 10:40 AM	9/23/2022 4:43 PM		
			N/A		HITRUST - Castle Greyskull (| | [r2])	0001.0	0101.00a1Organizational.123	💬			8/20/2020 12:34 PM			
			N/A		HITRUST - 4/6 Test (| | [r2])	0001.0	0101.00a1Organizational.123	💬			5/3/2021 11:48 AM			
N/A	N/A	Internal	N/A		HITRUST - Castle Greyskull (| | [r2])	0297.0	0104.02a1Organizational.12	💬			8/20/2020 12:33 PM			
N/A	N/A	Internal	N/A		HITRUST - z-Resource for Monitoring RS (| | [r2])	0999.0	0301.09o1Organizational.123	💬			2/17/2022 10:07 AM			

HITRUST 2022 COLLABORATE

Internal & *External* **Inheritance** – Creating / Submitting Requests (via Offline Template) **by Assessed Entity**

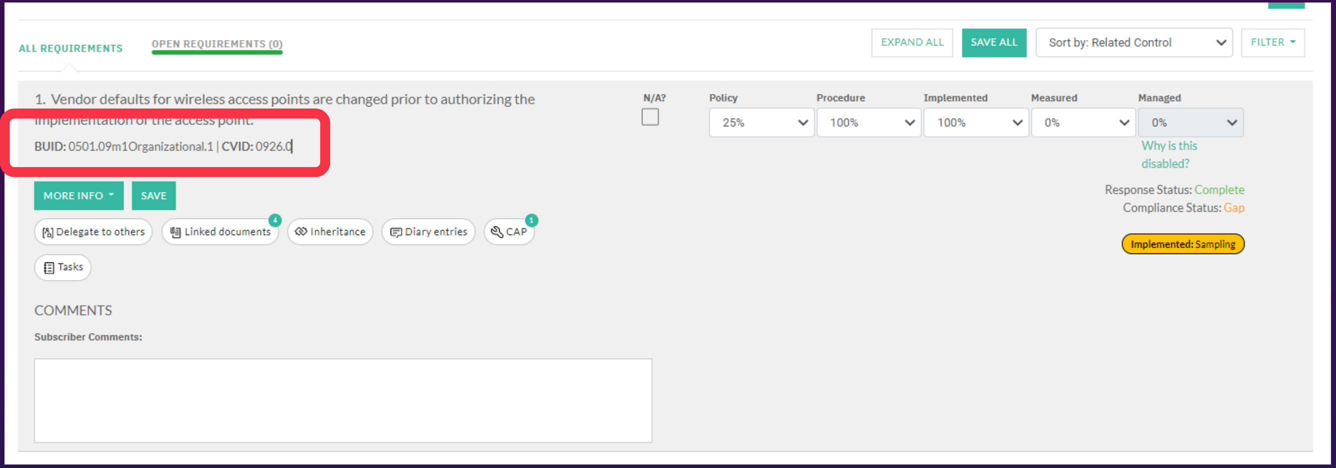
- New inheritance enhancement adds inheritance functionality to the Offline Assessment Template (MyCSF Release 1.16)
  - Supports both internal and external inheritance
  - Streamlines assessment process by allowing inheritance to be requested/applied in bulk
  - Includes enhanced data import error reporting and user guidance



	B	C	D	E
1	Request Status	Baseline Unique ID	Inherited Assessment	Weight (%)
2	Applied	0101.00a1Organizational.123	HITRUST / Castle Greyskull	-1
3	Applied	0101.00a1Organizational.123	HITRUST / 4/6 Test	-1
4	Applied	0104.02a1Organizational.12	HITRUST / Castle Greyskull	-1
5	Applied	0301.09o1Organizational.123	HITRUST / z-Resource for Monitoring RS	-1
6	Submitted	0101.00a1Organizational.123	SOFTWARE_QC / SSRS_Test_FinalReportUpload	100
7	Created	0210.01g1Organizational.1	SOFTWARE_QC / SSRS_Test_FinalReportUpload	75
8	Created	0211.01g1Organizational.2	SOFTWARE_QC / SSRS_Test_FinalReportUpload	50
9				

CVID-Enable Inheritance

- New inheritance enhancement changes the logic to use the CVID for cross-version inheritance instead of the BUID (MyCSF Release 15)
    - Fixes the incorrect control matches with same BUID that should break cross-version inheritance
    - Enables cross-version for INTERNAL inheritance
    - Improves transparency of HITRUST CSF control lifecycle
    - Expands inheritability of other duplicate controls via new CVID matching table administrative tool
    - Control requirement's CVID/BUID pair now visible in the MyCSF assessment objects/library & HITRUST SRMs



1. Vendor defaults for wireless access points are changed prior to authorizing the implementation of the access point.

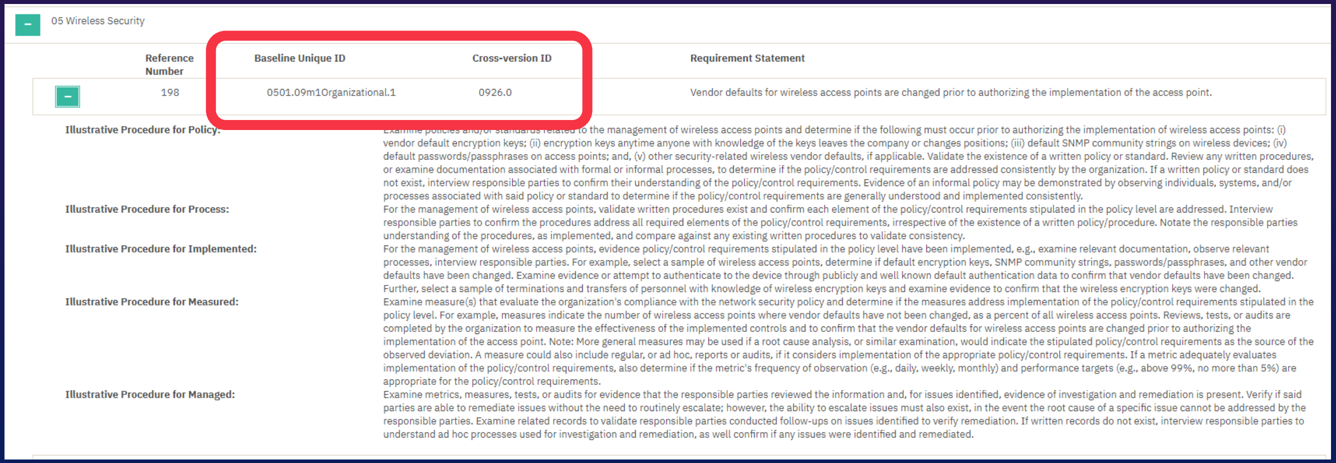
BUID: 0501.09m1Organizational.1 | **CVID:** 0926.0

N/A?	Policy	Procedure	Implemented	Measured	Managed
□	25%	100%	100%	0%	0%

Response Status: Complete
Compliance Status: Gap

COMMENTS

Subscriber Comments:



05 Wireless Security

	Reference Number	Baseline Unique ID	Cross-version ID	Requirement Statement
−	198	0501.09m1Organizational.1	0926.0	Vendor defaults for wireless access points are changed prior to authorizing the implementation of the access point.

Illustrative Procedure for Policy: Examine policies and/or standards related to the management of wireless access points and determine if the following must occur prior to authorizing the implementation of wireless access points: (i) vendor default encryption keys; (ii) encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions; (iii) default SNMP community strings on wireless devices; (iv) default passwords/passphrases on access points; and, (v) other security-related wireless vendor defaults, if applicable. Validate the existence of a written policy or standard. Review any written procedures, or examine documentation associated with formal or informal processes, to determine if the policy/control requirements are addressed consistently by the organization. If a written policy or standard does not exist, interview responsible parties to confirm their understanding of the policy/control requirements. Evidence of an informal policy may be demonstrated by observing individuals, systems, and/or processes associated with said policy or standard to determine if the policy/control requirements are generally understood and implemented consistently.

Illustrative Procedure for Process: For the management of wireless access points, validate written procedures exist and confirm each element of the policy/control requirements stipulated in the policy level are addressed. Interview responsible parties to confirm the procedures address all required elements of the policy/control requirements, irrespective of the existence of a written policy/procedure. Notate the responsible parties understanding of the procedures, as implemented, and compare against any existing written procedures to validate consistency.

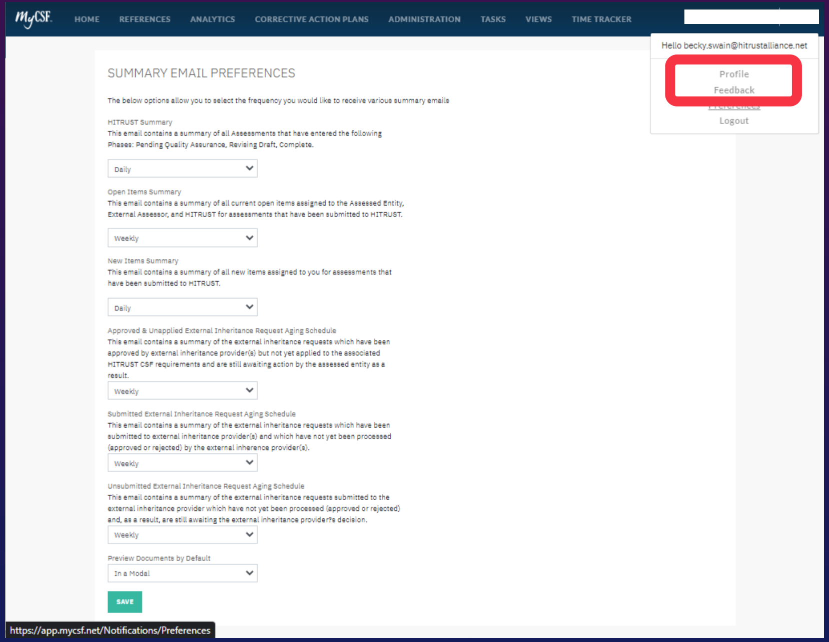
Illustrative Procedure for Implemented: For the management of wireless access points, evidence policy/control requirements stipulated in the policy level have been implemented, e.g., examine relevant documentation, observe relevant processes, interview responsible parties. For example, select a sample of wireless access points, determine if default encryption keys, SNMP community strings, passwords/passphrases, and other vendor defaults have been changed. Examine evidence or attempt to authenticate to the device through publicly and well known default authentication data to confirm that vendor defaults have been changed. Further, select a sample of terminations and transfers of personnel with knowledge of wireless encryption keys and examine evidence to confirm that the wireless encryption keys were changed.

Illustrative Procedure for Measured: Examine measure(s) that evaluate the organization's compliance with the network security policy and determine if the measures address implementation of the policy/control requirements stipulated in the policy level. For example, measures indicate the number of wireless access points where vendor defaults have not been changed, as a percent of all wireless access points. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the vendor defaults for wireless access points are changed prior to authorizing the implementation of the access point. Note: More general measures may be used if a root cause analysis, or similar examination, would indicate the stipulated policy/control requirements as the source of the observed deviation. A measure could also include regular, or ad hoc, reports or audits, if it considers implementation of the appropriate policy/control requirements. If a metric adequately evaluates implementation of the policy/control requirements, also determine if the metric's frequency of observation (e.g., daily, weekly, monthly) and performance targets (e.g., above 99%, no more than 5%) are appropriate for the policy/control requirements.

Illustrative Procedure for Managed: Examine metrics, measures, tests, or audits for evidence that the responsible parties reviewed the information and, for issues identified, evidence of investigation and remediation is present. Verify if said parties are able to remediate issues without the need to routinely escalate; however, the ability to escalate issues must also exist, in the event the root cause of a specific issue cannot be addressed by the responsible parties. Examine related records to validate responsible parties conducted follow-ups on issues identified to verify remediation. If written records do not exist, interview responsible parties to understand ad hoc processes used for investigation and remediation, as well confirm if any issues were identified and remediated.

External Inheritance – Enhanced Status Reporting for **Inheritance Providers** / **Assessed Entities**

- New configurable email notifications with inheritance request aging schedules in user preferences (MyCSF Release 1.15)



SUMMARY EMAIL PREFERENCES

The below options allow you to select the frequency you would like to receive various summary emails

HITRUST Summary
This email contains a summary of all Assessments that have entered the following Phases: Pending Quality Assurance, Revising Draft, Complete.

Daily

Open Items Summary
This email contains a summary of all current open items assigned to the Assessed Entity, External Assessor, and HITRUST for assessments that have been submitted to HITRUST.

Weekly

New Items Summary
This email contains a summary of all new items assigned to you for assessments that have been submitted to HITRUST.

Daily

Approved & Unapplied External Inheritance Request Aging Schedule
This email contains a summary of the external inheritance requests which have been approved by external inheritance provider(s) but not yet applied to the associated HITRUST CSF requirements and are still awaiting action by the assessed entity as a result.

Weekly

Submitted External Inheritance Request Aging Schedule
This email contains a summary of the external inheritance requests which have been submitted to external inheritance provider(s) and which have not yet been processed (approved or rejected) by the external inherence provider(s).

Weekly

Unsubmitted External Inheritance Request Aging Schedule
This email contains a summary of the external inheritance requests submitted to the external inheritance provider which have not yet been processed (approved or rejected) and, as a result, are still awaiting the external inheritance provider?s decision.

Weekly

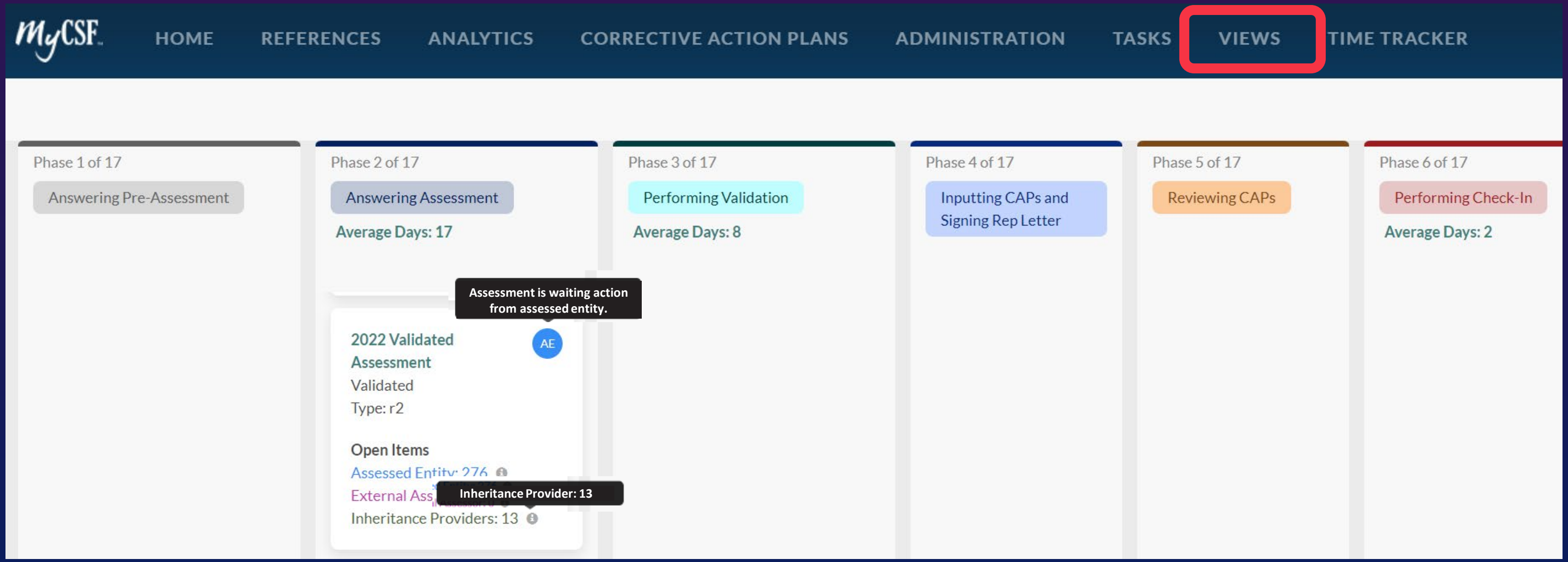
Preview Documents by Default

In a Modal

SAVE

https://app.mycsf.net/Notifications/Preferences

- Pending inheritance requests added to Kanban Board (MyCSF Release 1.15)



Phase 1 of 17
Answering Pre-Assessment

Phase 2 of 17
Answering Assessment
Average Days: 17

Phase 3 of 17
Performing Validation
Average Days: 8

Phase 4 of 17
Inputting CAPs and Signing Rep Letter

Phase 5 of 17
Reviewing CAPs

Phase 6 of 17
Performing Check-In
Average Days: 2

Assessment is waiting action from assessed entity.

2022 Validated Assessment
AE
Validated
Type: r2

Open Items
Assessed Entity: 276
External Ass
Inheritance Provider: 13
Inheritance Providers: 13

External Inheritance – General User Guidance for **the Assessed Entity**

- Assessed Entities should work closely with their External Assessor team when utilizing external inheritance (and/or contact your HITRUST CSM/Support for further assistance) and use the following as a step-by-step guideline…

STEP 1

The Assessed Entity has confirmed as having a ***valid business justification*** for utilizing external inheritance by meeting HITRUST's Subscriber & CSF Assurance requirements qualifications (listed on next slide).

STEP 2

The Assessed Entity has a ***rationalized approach*** for weighting external inheritance requests that was derived with input from:

(a) The HITRUST SRM to determine the inheritability values of controls (SRM Type)
AND

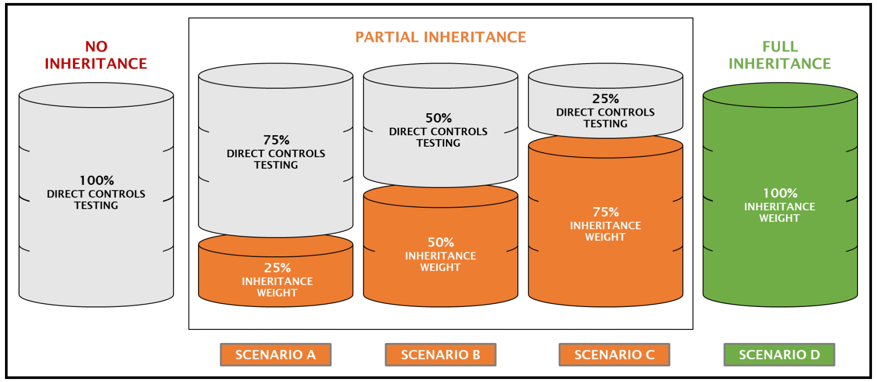
(b) Understanding of what portion of the assessment scope is reasonably covered by the third-party organization's common HITRUST CSF controls.

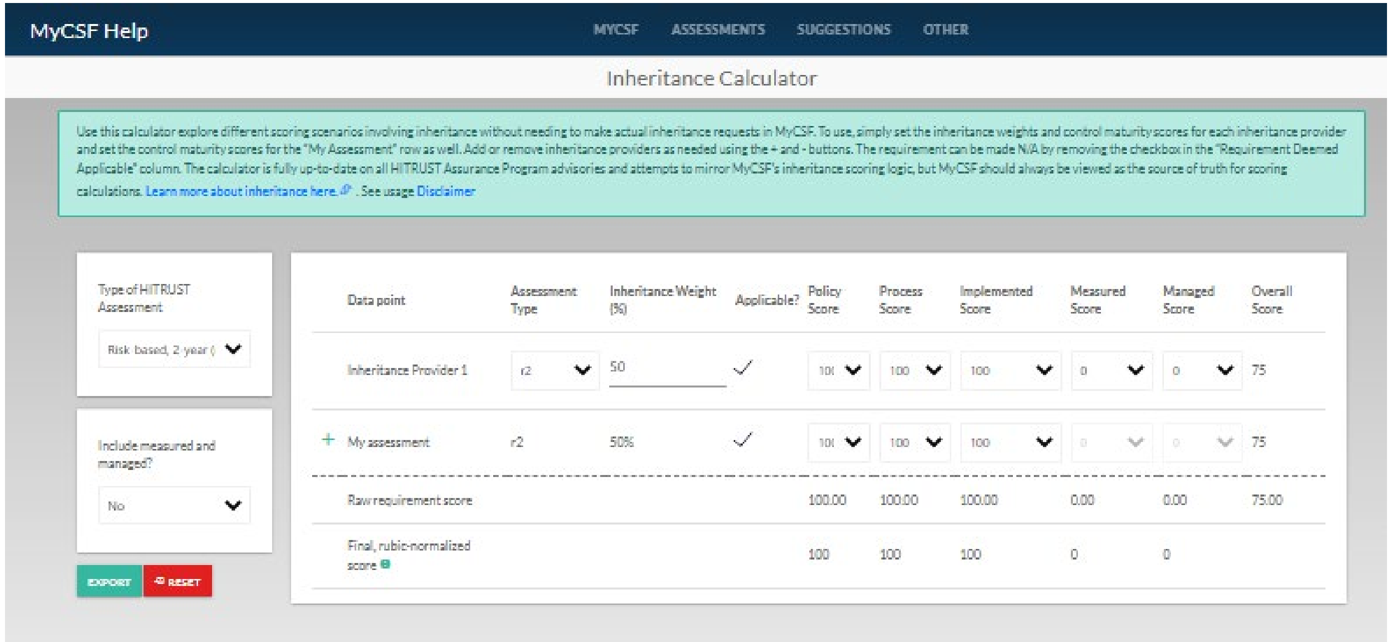
HITRUST Customer Qualifications: Assessed Entity

Type	Description
MyCSF Subscription	• INTERNAL INHERITANCE: Assessment owner is an active annual MyCSF subscriber with a Corporate or Premier-level subscription. • EXTERNAL INHERITANCE: Assessment owner is an active annual MyCSF subscriber with a Professional, Corporate or Premier-level subscription.
HITRUST Assurance Requirements	EXTERNAL INHERITANCE (ONLY): • There exists a valid business justification for the Assessed Entity, as a relying party, to request External Inheritance by qualifying for both of the following scoping conditions: ✓ Inheriting assessment type—The assessment is a supported HITRUST Validated or Readiness Assessment type that allows use of External Inheritance. ✓ Customer verification—The Assessed Entity is an active customer of the Inheritance Provider with a direct contractual arrangement in place (still in good standing) that can be verified by the Inheritance Provider. ✓ Common assessment scope—The inheriting assessment scope boundary includes the Inheritance Provider's products/services and associated common CSF control requirements covered by the inheritable assessment scope. • Inheritance requests are submitted to the Inheritance Provider for approval and applied before the end of the 90-day assessment testing period (including consenting to terms/conditions for inheritance-related sharing/exchange of privileged customer information).

External Inheritance – General User Guidance for **the Assessed Entity** (cont.)

- Partial inheritance (with 1 < x < 99% weight) can be nuanced/complex but helped by using the new **Inheritance Calculator** assessment tool now available on MyCSF Help via https://help.mycsf.net/inheritance-calc/
  - **Scenario A:** 25% weight of control inheritability
  - **Scenario B:** 50% weight of control inheritability
  - **Scenario C:** 75% weight of control inheritability
  - **Scenario D:** 100% weight of control inheritability





Inheritance Calculator

Use this calculator explore different scoring scenarios involving inheritance without needing to make actual inheritance requests in MyCSF. To use, simply set the inheritance weights and control maturity scores for each inheritance provider and set the control maturity scores for the "My Assessment" row as well. Add or remove inheritance providers as needed using the + and - buttons. The requirement can be made N/A by removing the checkbox in the "Requirement Deemed Applicable" column. The calculator is fully up-to-date on all HITRUST Assurance Program advisories and attempts to mirror MyCSF's inheritance scoring logic, but MyCSF should always be viewed as the source of truth for scoring calculations. Learn more about inheritance here. . See usage Disclaimer

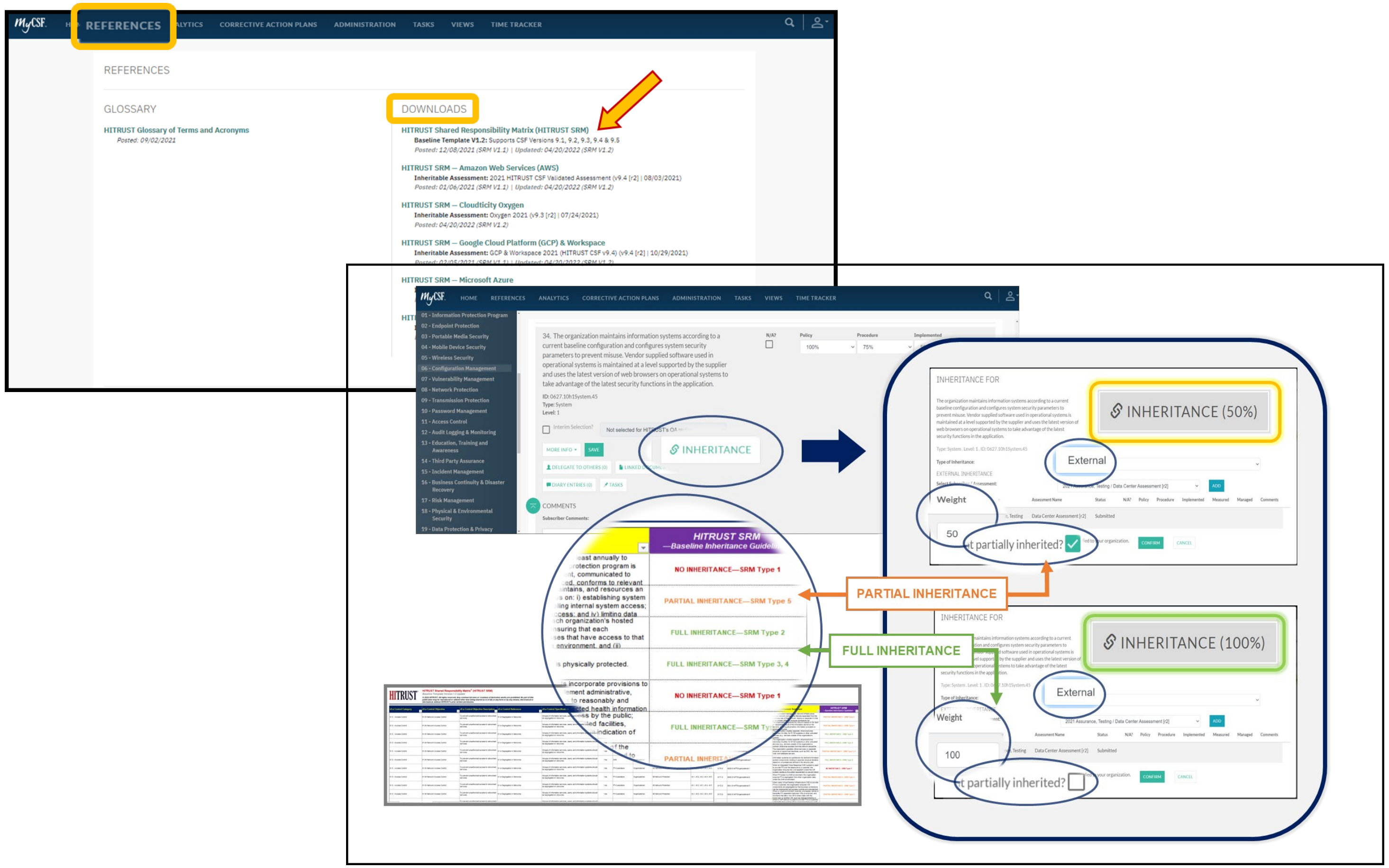
Type of HITRUST Assessment: Risk based, 2 year (

Include measured and managed?: No

Data point	Assessment Type	Inheritance Weight (%)	Applicable?	Policy Score	Process Score	Implemented Score	Measured Score	Managed Score	Overall Score
Inheritance Provider 1	r2	50	✓	10(	100	100	0	0	75
+ My assessment	r2	50%	✓	10(	100	100	0	0	75
Raw requirement score				100.00	100.00	100.00	0.00	0.00	75.00
Final, rubic-normalized score				100	100	100	0	0	

External Inheritance – General User Guidance for **the Assessed Entity** (cont.)

- The HITRUST SRM is an essential guideline for determining the inheritability values of external controls based on SRM Type
- Assessed Entities can download the HITRUST SRMs tailored for Inheritance Providers, or if unavailable, use HITRUST's baseline template
- ***Important*** to keep in mind:
  - Not all control requirements should be inherited (i.e., SRM Type 1 controls)
  - Not all control requirements should be fully inherited (with 100% weight)



HITRUST Glossary of Terms and Acronyms
Posted: 09/02/2021

HITRUST Shared Responsibility Matrix (HITRUST SRM)
Baseline Template V1.2: Supports CSF Versions 9.1, 9.2, 9.3, 9.4 & 9.5
Posted: 12/08/2021 (SRM V1.1) | Updated: 04/20/2022 (SRM V1.2)

HITRUST SRM – Amazon Web Services (AWS)
Inheritable Assessment: 2021 HITRUST CSF Validated Assessment (v9.4 [r2] | 08/03/2021)
Posted: 01/06/2021 (SRM V1.1) | Updated: 04/20/2022 (SRM V1.2)

HITRUST SRM – Cloudticity Oxygen
Inheritable Assessment: Oxygen 2021 (v9.3 [r2] | 07/24/2021)
Posted: 04/20/2022 (SRM V1.2)

HITRUST SRM – Google Cloud Platform (GCP) & Workspace
Inheritable Assessment: GCP & Workspace 2021 (HITRUST CSF v9.4) (v9.4 [r2] | 10/29/2021)

HITRUST SRM – Microsoft Azure

34. The organization maintains information systems according to a current baseline configuration and configures system security parameters to prevent misuse. Vendor supplied software used in operational systems is maintained at a level supported by the supplier and uses the latest version of web browsers on operational systems to take advantage of the latest security functions in the application.
ID: 0627.10h1System.45
Type: System
Level: 1

Policy: 100%
Procedure: 75%

Weight: 50
Data Center Assessment [r2] Submitted
...t partially inherited? ☑

Weight: 100
2021 Assurance, Testing / Data Center Assessment [r2]
Data Center Assessment [r2] Submitted
...t partially inherited? □

The HITRUST Shared Responsibility Matrix® (SRM) – Baseline Template

- Resolves ***cloudy*** uncertainty and ambiguity by clearly defining how to rely on shared information security and privacy controls
- Built on the first vendor-agnostic ***shared responsibility model*** suited for shared cloud-hosted platforms and application services
- Provides an out-of-box blueprint with pre-populated inheritability values, referred to as ***SRM Types***, assigned to over 2,000 HITRUST CSF control requirements
- Tailored for HITRUST's **Inheritance Providers** as a benefit for their relying customers to download from HITRUST's website or via MyCSF.

Inheritability Value	Applicable SRM Type(s)
NO INHERITANCE *(0% weight)*	**SRM Type 1** – *Entity-Level / Organizational Internal Controls*
PARTIAL INHERITANCE *(1 < x < 99% weight)*	**SRM Type 2** – *Third-Party Manual / Administrative Controls (Shared)*
	SRM Type 4 – *Technical / Automated Controls (Tangible)*
	SRM Type 5 – *Technical / Automated Controls (Intangible)*
FULL INHERITANCE *(100% weight)*	**SRM Type 2** – *Third-Party Manual / Administrative Controls (Not Shared)*
	SRM Type 3 – *Physical Access / Environmental Security Controls*

HITRUST SRM – Baseline Template:
External Controls Inheritability Values (SRM Types)

SRM Type	Definition
SRM Type 1 *Entity-Level / Organizational Internal Controls*	The control is **NOT INHERITABLE** if no portion of the control must involve or be shared with/outsourced to another third-party organization as a material dependency for the assessed entity to sufficiently perform and the external assessor to validate implementation of the control (note: these controls may be internally inheritable). Example control activities: • Entity-level/organizational policies, programs, and processes • User personnel conduct or HR-related involving personnel on/off-boarding and training • Internal use of corporate/shared IT services • Scope limited to only locally-hosted or on-prem sites and facilities, including remote or teleworker locations, that do not share technical interfaces and/or remote user access or network connectivity involving technologies or user personnel belonging to the third-party organization

HITRUST SRM – Baseline Template:
External Controls Inheritability Values (SRM Types)

SRM Type	Definition
SRM Type 2 *Third-Party Manual / Administrative Controls*	The control may qualify for **PARTIAL INHERITANCE** if a partial portion or **FULL INHERITANCE** if a total portion of the control must involve or be shared with/outsourced to another third-party organization as a material dependency for the assessed entity to sufficiently perform (and the external assessor to validate) implementation of the control AND the control can be characterized as having administrative or manual processing qualities that require some form or element of action taken by user personnel belonging to the third-party organization. Example control activities: • Vendor, supplier, or cyber supply-chain or other related risk and assurance activities • Service contracting or other forms of legal arrangements • Joint privacy compliance obligations between covered entities/business associates or data controllers/processors

HITRUST SRM – Baseline Template:
External Controls Inheritability Values (SRM Types)

SRM Type	Definition
SRM Type 3 *Physical Access / Environmental Security Controls*	The control may qualify for **FULL INHERITANCE** if a total portion of the control must involve or be shared with/outsourced to another third-party organization as a material dependency for the assessed entity to sufficiently perform (and the external assessor to validate) implementation of the control AND the control can be characterized as having physical qualities that require some form or element of action taken by user personnel belonging to the third-party organization. Example control activities: • Involves provisioning and controlling of user access or use of environmental security measure for protection of off-prem or collocated facilities, or facilities that host external third-party services, i.e., SaaS-based mobile or web applications, shared cloud infrastructures/platforms (IaaS/PaaS), and datacenter hosting services

HITRUST SRM – Baseline Template:
External Controls Inheritability Values (SRM Types)

SRM Type	Definition
SRM Type 4 *Technical / Automated Controls (Tangible)*	The control may qualify for **PARTIAL INHERITANCE** if a partial portion or **FULL INHERITANCE** if a total portion of the control must involve or be shared with/outsourced to another third-party organization as a material dependency for the assessed entity to sufficiently perform (and the external assessor to validate) implementation of the control AND the control can be characterized as having both physical and technical qualities that require some form or element of action taken by user personnel belonging to the third-party organization. Example control activities: • Involves placement, treatment, handling, configuration, or use of tangible forms of portable/mobile or stationary hardware-based technologies or other forms of system component, cabling or equipment located off-prem but may share technical interfaces and/or remote user access or network connectivity involving technologies or user personnel belonging to the assessed entity

HITRUST SRM – Baseline Template:
External Controls Inheritability Values (SRM Types)

SRM Type	Definition
SRM Type 5 *Technical / Automated Controls (Intangible)*	The control may qualify for **PARTIAL INHERITANCE** if a partial portion or **FULL INHERITANCE** if a total portion of the control must involve or be shared with/outsourced to another third-party organization as a material dependency for the assessed entity to sufficiently perform (and the external assessor to validate) implementation of the control AND the control can be characterized as having logical or automated technical qualities that require some form or element of action taken by user personnel belonging to the third-party organization. Example control activities: • Involves placement, treatment, handling, configuration, or use of tangible forms of portable/mobile or stationary hardware-based technologies or other forms of system component, cabling or equipment located off-prem but may share technical interfaces and/or remote user access or network connectivity involving technologies or user personnel belonging to the assessed entity

HITRUST 2022
COLLABORATE

Thank You For Attending!