HITRUST

AI Elements in HITRUST CSF v11.2.0

02/28/24

HITRUST AI Initiative Overview

HITRUST AI Initiative

HITRUST is leading the way with an industry first AI Assurance program, which will result in a certification and easily consumable insight report. Working with industry leaders, we have adopted emerging AI frameworks and tailored control requirements to work within MyCSF as part of an existing assessment of information security controls to reduce overall effort, and provide a level of assurance over AI risk in addition to sound security practices.

This presentation will show you how to use the CSF and/or MyCSF to begin utilizing AI risk management controls in your organization, and stage for success as new deliverables such as a HITRUST AI certification and insight reports are brought out.

Additionally, AI security controls will be introduced for later versions of the HITRUST CSF as those controls are identified and solidified among AI pioneers.

HITRUST CSF v11.20 AI Authoritative Sources

Currently, AI mappings to the following are included

- NIST AI RMF 1.0
- ISO 23894
- Also included as relevant AI mapping are controls from ISO 31000

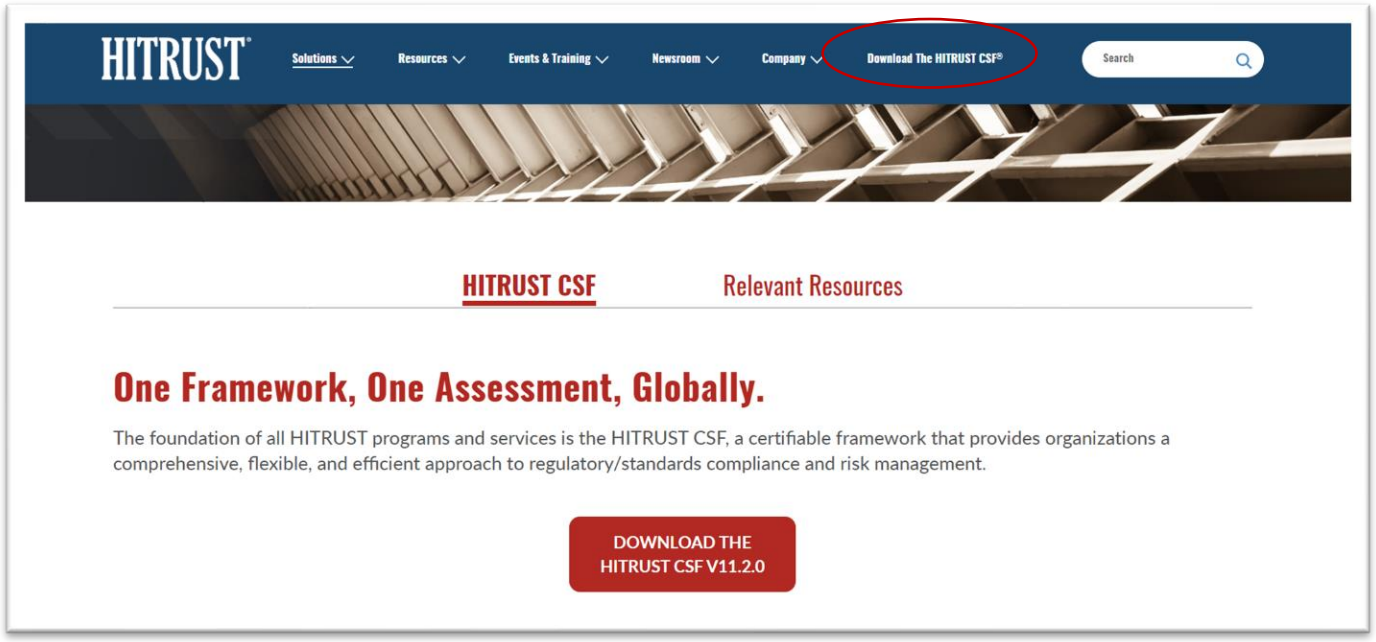
Overall, there are over 300 AI relevant mappings, with up to 50 unique requirements included when selecting the AI compliance factor in MyCSF assessments.

Using the HITRUST CSF to Identify AI Controls

HITRUST CSF AI Control Identification

The HITRUST CSF version 11.20 download package contains a PDF of the CSF, in addition to an authoritative source cross reference and introduction document. Organizations can easily download the HITRUST CSF and utilize the framework free of charge for qualified organizations whose primary use will be to use the framework for their organization.

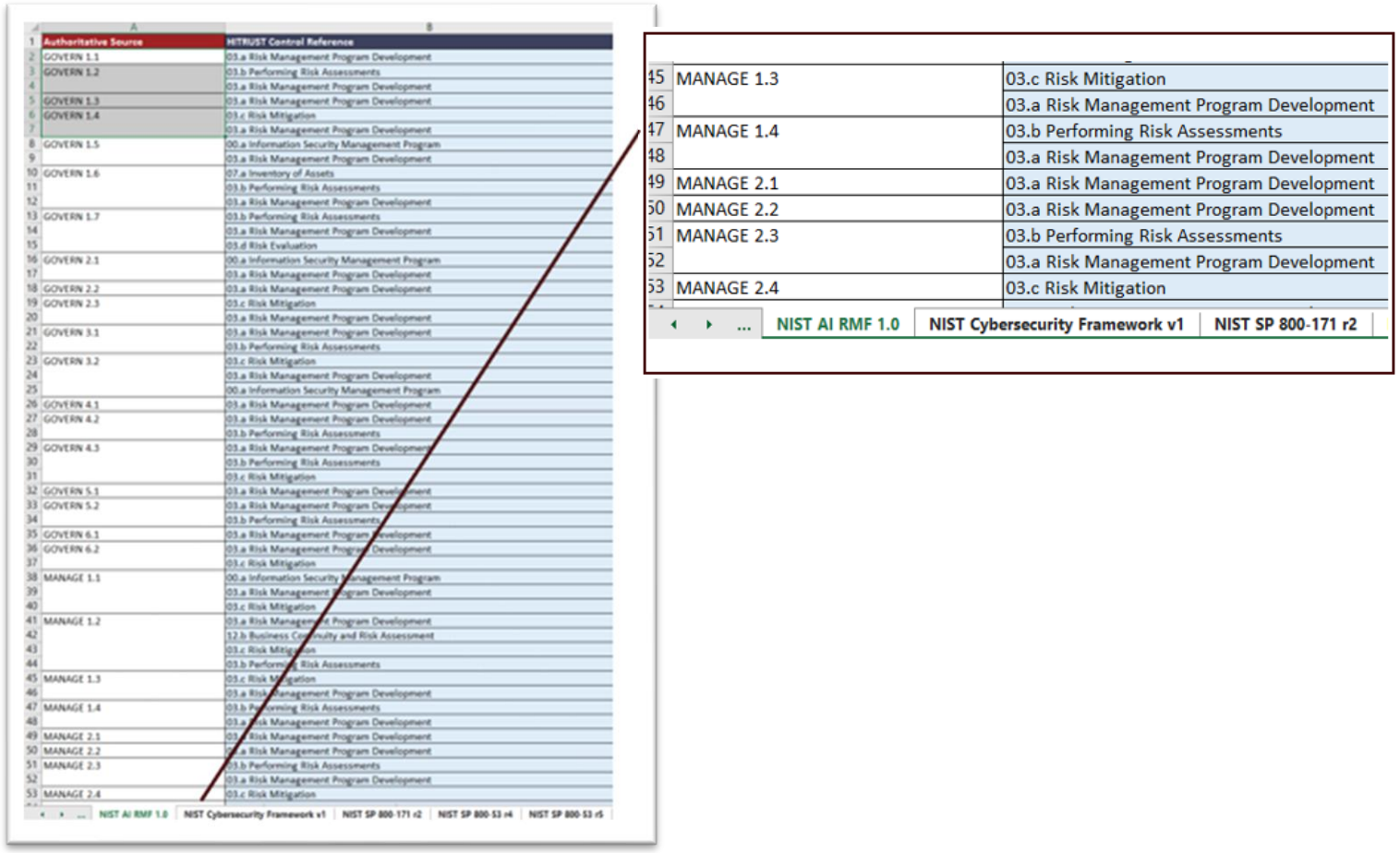
Downloading the HITRUST CSF



Downloading the HITRUST CSF is easy.

- Go to our website hitrustalliance.net
- Follow the prompts from the top navigation to Download the CSF

Understanding the CSF to Identify AI Controls



	A	B
1	Authoritative Source	HITRUST Control Reference
2	GOVERN 1.1	03.a Risk Management Program Development
3	GOVERN 1.2	03.b Performing Risk Assessments
4		03.a Risk Management Program Development
5	GOVERN 1.3	03.a Risk Management Program Development
6	GOVERN 1.4	03.c Risk Mitigation
7		03.a Risk Management Program Development
8	GOVERN 1.5	00.a Information Security Management Program
9		03.a Risk Management Program Development
10	GOVERN 1.6	07.a Inventory of Assets
11		03.b Performing Risk Assessments
12		03.a Risk Management Program Development
13	GOVERN 1.7	03.b Performing Risk Assessments
14		03.a Risk Management Program Development
15		03.d Risk Evaluation
16	GOVERN 2.1	00.a Information Security Management Program
17		03.a Risk Management Program Development
18	GOVERN 2.2	03.a Risk Management Program Development
19	GOVERN 2.3	03.c Risk Mitigation
20		03.a Risk Management Program Development
21	GOVERN 3.1	03.a Risk Management Program Development
22		03.b Performing Risk Assessments
23	GOVERN 3.2	03.c Risk Mitigation
24		03.a Risk Management Program Development
25		00.a Information Security Management Program
26	GOVERN 4.1	03.a Risk Management Program Development
27	GOVERN 4.2	03.a Risk Management Program Development
28		03.b Performing Risk Assessments
29	GOVERN 4.3	03.a Risk Management Program Development
30		03.b Performing Risk Assessments
31		03.c Risk Mitigation
32	GOVERN 5.1	03.a Risk Management Program Development
33	GOVERN 5.2	03.a Risk Management Program Development
34		03.b Performing Risk Assessments
35	GOVERN 6.1	03.a Risk Management Program Development
36	GOVERN 6.2	03.a Risk Management Program Development
37		03.c Risk Mitigation
38	MANAGE 1.1	00.a Information Security Management Program
39		03.a Risk Management Program Development
40		03.c Risk Mitigation
41	MANAGE 1.2	03.a Risk Management Program Development
42		12.b Business Continuity and Risk Assessment
43		03.c Risk Mitigation
44		03.b Performing Risk Assessments
45	MANAGE 1.3	03.c Risk Mitigation
46		03.a Risk Management Program Development
47	MANAGE 1.4	03.b Performing Risk Assessments
48		03.a Risk Management Program Development
49	MANAGE 2.1	03.a Risk Management Program Development
50	MANAGE 2.2	03.a Risk Management Program Development
51	MANAGE 2.3	03.b Performing Risk Assessments
52		03.a Risk Management Program Development
53	MANAGE 2.4	03.c Risk Mitigation

NIST AI RMF 1.0 | NIST Cybersecurity Framework v1 | NIST SP 800-171 r2 | NIST SP 800-53 r4 | NIST SP 800-53 r5

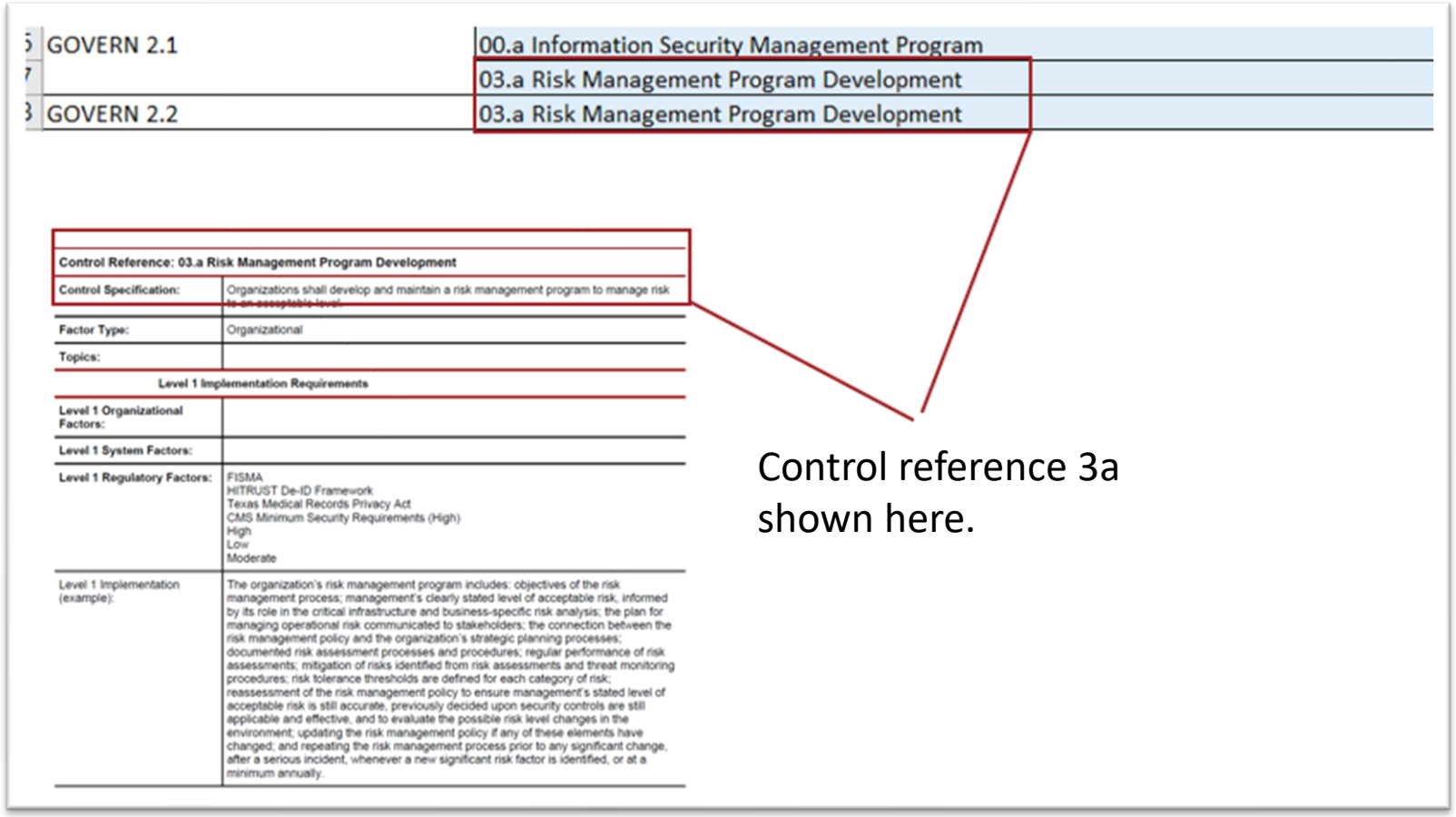
45	MANAGE 1.3	03.c Risk Mitigation
46		03.a Risk Management Program Development
47	MANAGE 1.4	03.b Performing Risk Assessments
48		03.a Risk Management Program Development
49	MANAGE 2.1	03.a Risk Management Program Development
50	MANAGE 2.2	03.a Risk Management Program Development
51	MANAGE 2.3	03.b Performing Risk Assessments
52		03.a Risk Management Program Development
53	MANAGE 2.4	03.c Risk Mitigation

... NIST AI RMF 1.0 | NIST Cybersecurity Framework v1 | NIST SP 800-171 r2

Starting with the **authoritative source cross reference**, navigate along the bottom tabs to the "NIST AI RMF 1.0".
This tab will contain the NIST AI RMF control areas mapped to HITRUST controls. Take note of the "HITRUST Control Reference" in column B.

HITRUST

Using the CSF to Identify AI Controls



GOVERN 2.1	00.a Information Security Management Program
	03.a Risk Management Program Development
GOVERN 2.2	03.a Risk Management Program Development

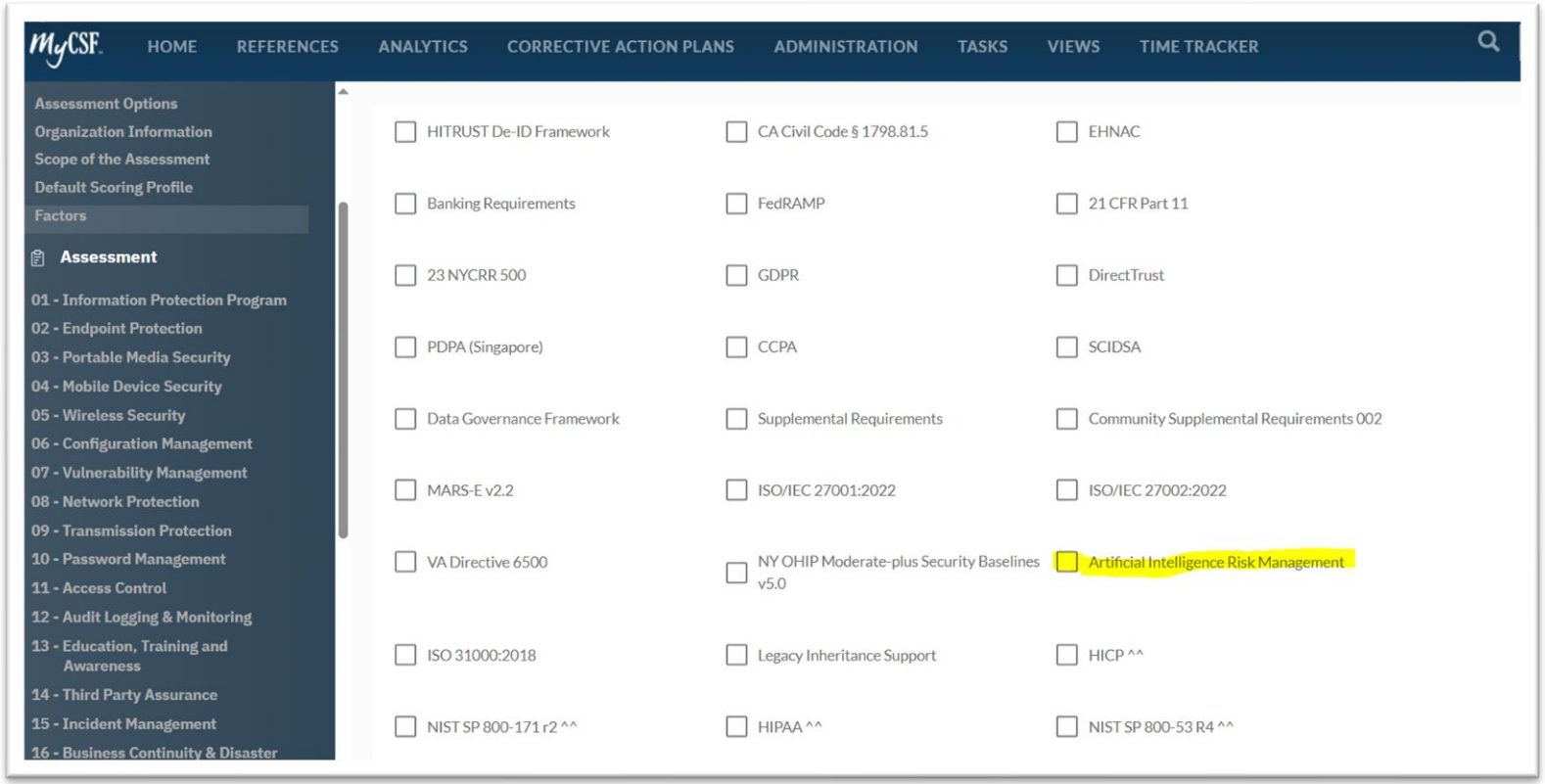
Control Reference: 03.a Risk Management Program Development	
Control Specification:	Organizations shall develop and maintain a risk management program to manage risk to an acceptable level.
Factor Type:	Organizational
Topics:	
Level 1 Implementation Requirements	
Level 1 Organizational Factors:	
Level 1 System Factors:	
Level 1 Regulatory Factors:	FISMA HITRUST De-ID Framework Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate
Level 1 Implementation (example):	The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.

Control reference 3a shown here.

Next, search the control reference in the HITRUST CSF PDF to see the relevant control text. There may be multiple strengths of control, use the guidance in the CSF to determine strength based on organizational, system, or regulatory factors.

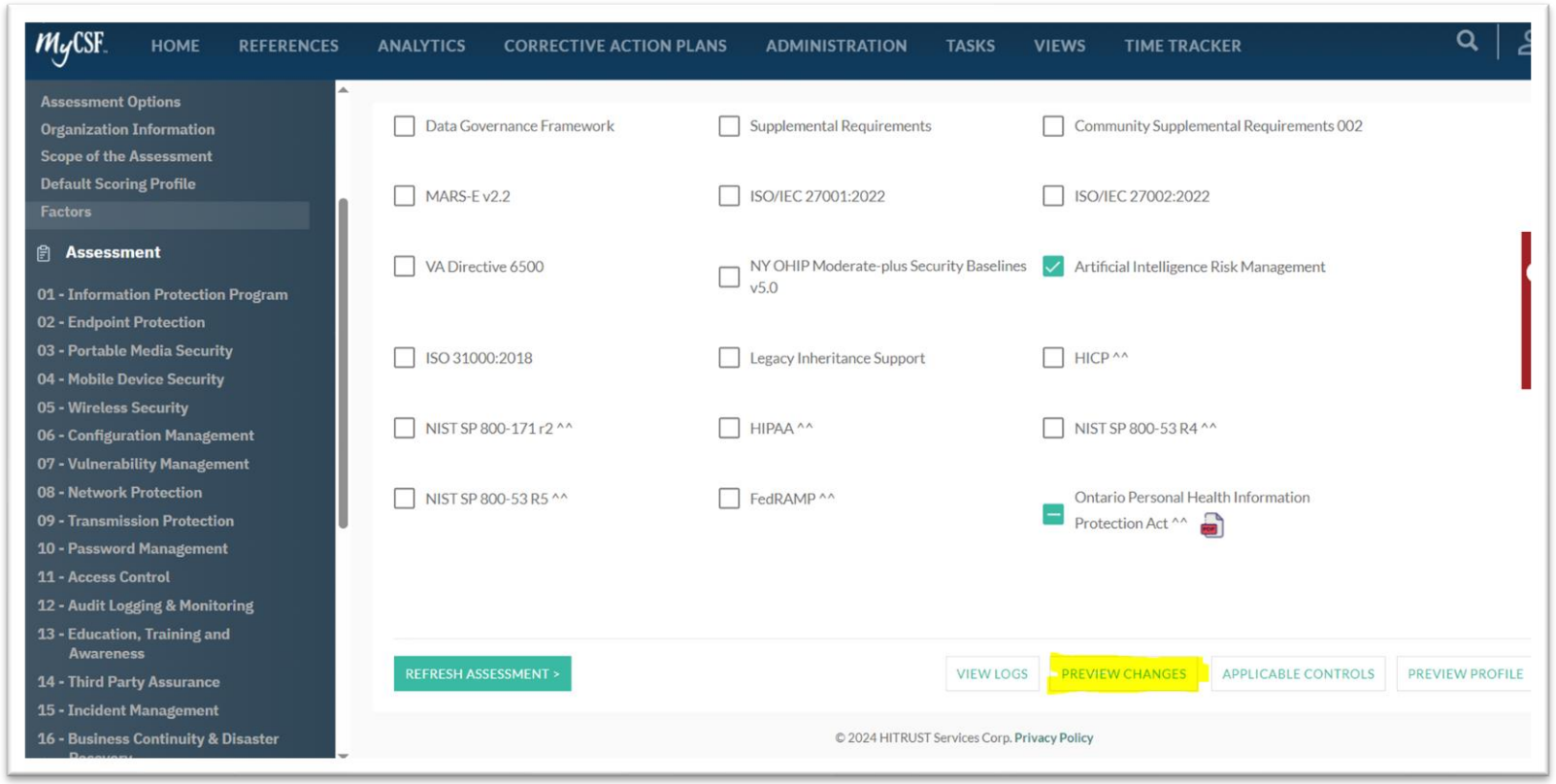
Using HITRUST MyCSF to Identify AI Controls

Using MyCSF – AI Compliance Factor on r2 Assessment



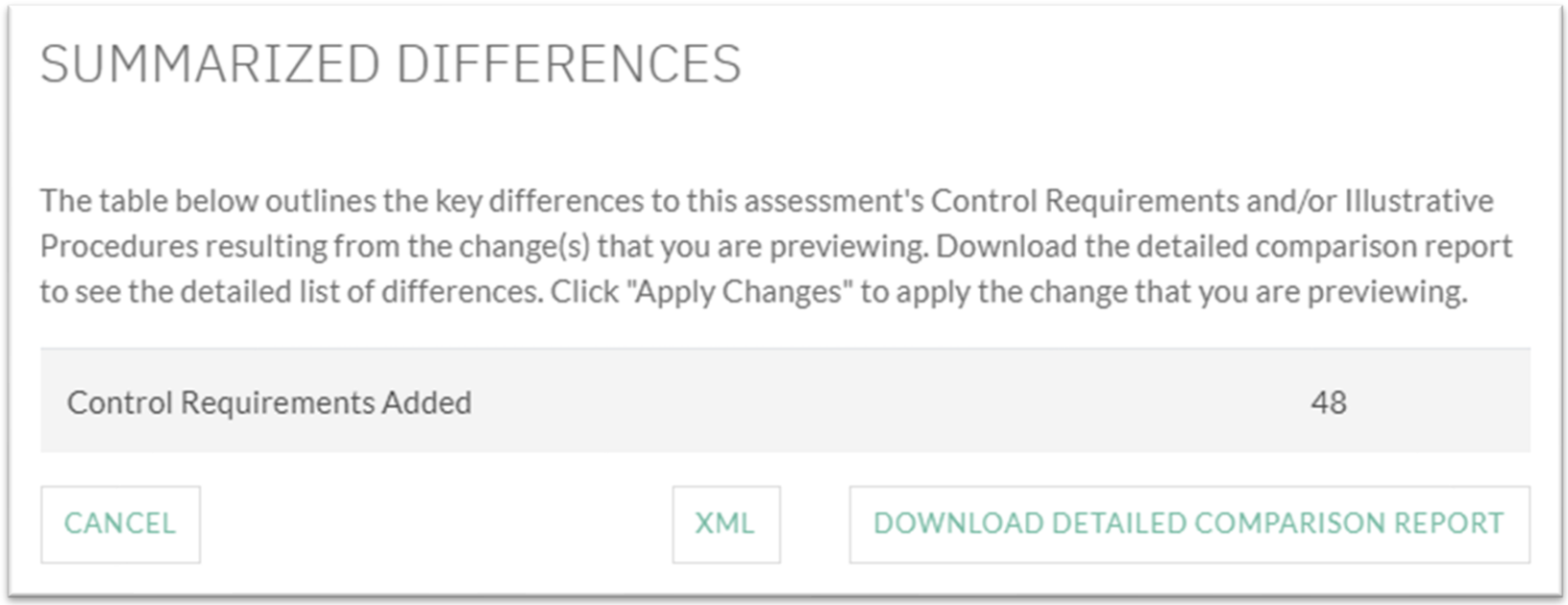
Organizations using an r2 assessment or a targeted assessment on v11.2 or later can choose to include the currently available controls identified by HITRUST and referencing NIST and ISO AI specifications.

Using MyCSF – AI Control Preview



These controls are available for review prior to inclusion in your assessment by selecting the “Preview Changes” function in MyCSF.

Using MyCSF – AI Control Preview



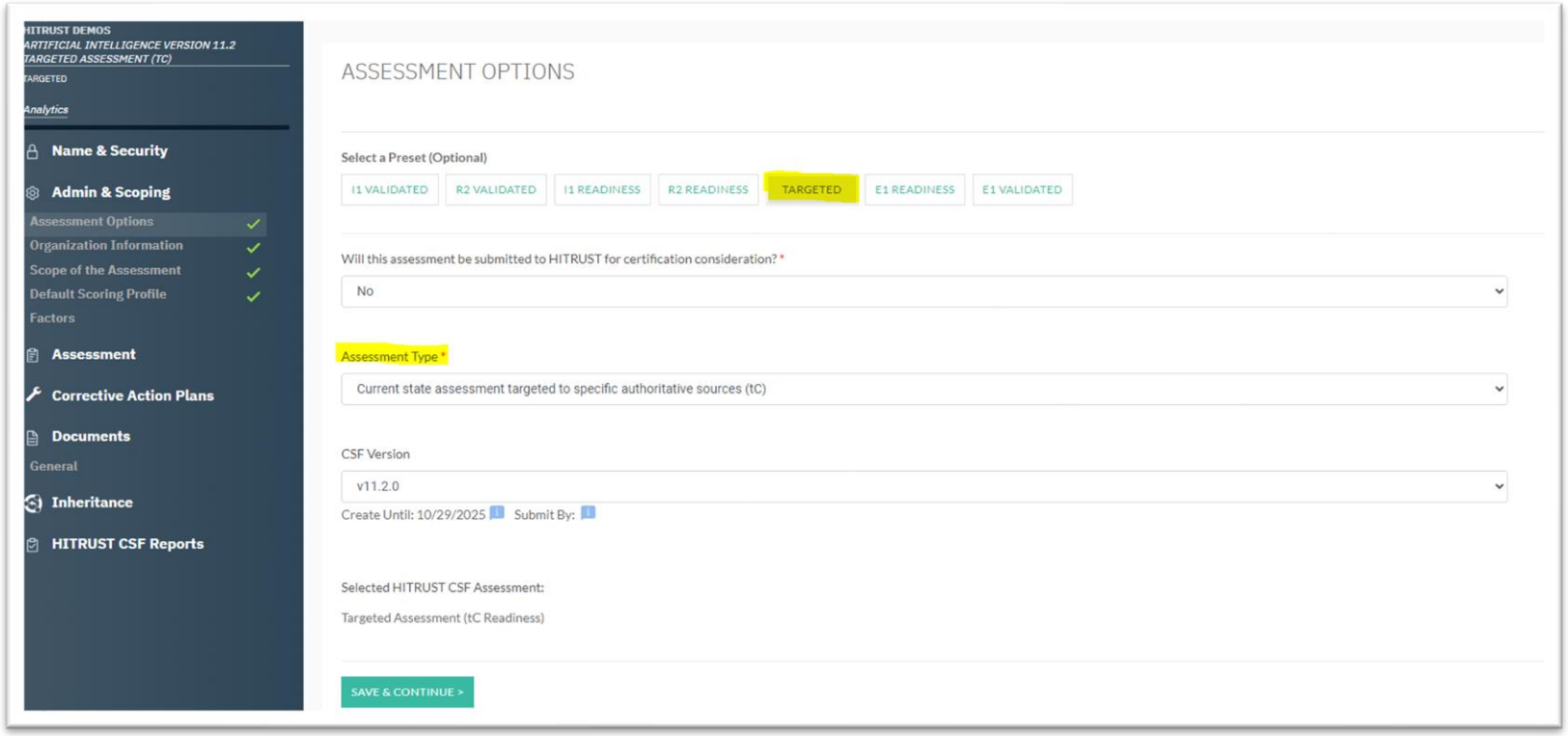
MyCSF will provide a quick view of the control changes in your selection, and if selected, you can apply the changes to your assessment. It also allows you to download a complete listing of the new requirements and mappings.

MyCSF – Control Preview Spreadsheet

Requirement ID	Area Impacted	Record Modified	Difference
			In support of the risk management process, the organization maintains documentation of the following aspects of the external context of organizations development and/or use of AI: relevant legal requirements, including those specifically relating to AI; guidelines on ethical use and design of AI and automated systems issued by government-related groups, regulators, standardization bodies, civil society, academia and industry associations; domain-specific guidelines and frameworks related to AI; technology trends and advancements in the various areas of AI; societal and political implications of the deployment of AI systems, including guidance from social sciences; external stakeholder perceptions, needs, and expectations; how the use of AI, especially AI systems using continuous learning, can affect the ability of the organization to meet contractual obligations and guarantees; contractual relationships during the design and production of AI systems and services; how the use of AI can increase the complexity of networks and dependencies; and how an AI system can replace an existing system and, in such a case, an assessment of the risk benefits and risk transfers of an AI system versus the existing system can be undertaken, considering safety, environmental, social, technical and financial issues associated with the implementation of the AI system.
01.03aISO23894Organizational.12	Assessment	Control Requirement Added	
01.03aISO23894Organizational.12	Library	Mapping Added	ISO/IEC 23894:2023\5.4.1
01.03aISO23894Organizational.12	Library	Mapping Added	NIST AI RMF 1.0\GOVERN 1.1
01.03aISO23894Organizational.12	Library	Mapping Added	NIST AI RMF 1.0\GOVERN 2.2
01.03aISO23894Organizational.12	Library	Mapping Added	NIST AI RMF 1.0\GOVERN 4.1

This view shows the added, removed, or modified control requirements and mappings based on the AI factor inclusion.

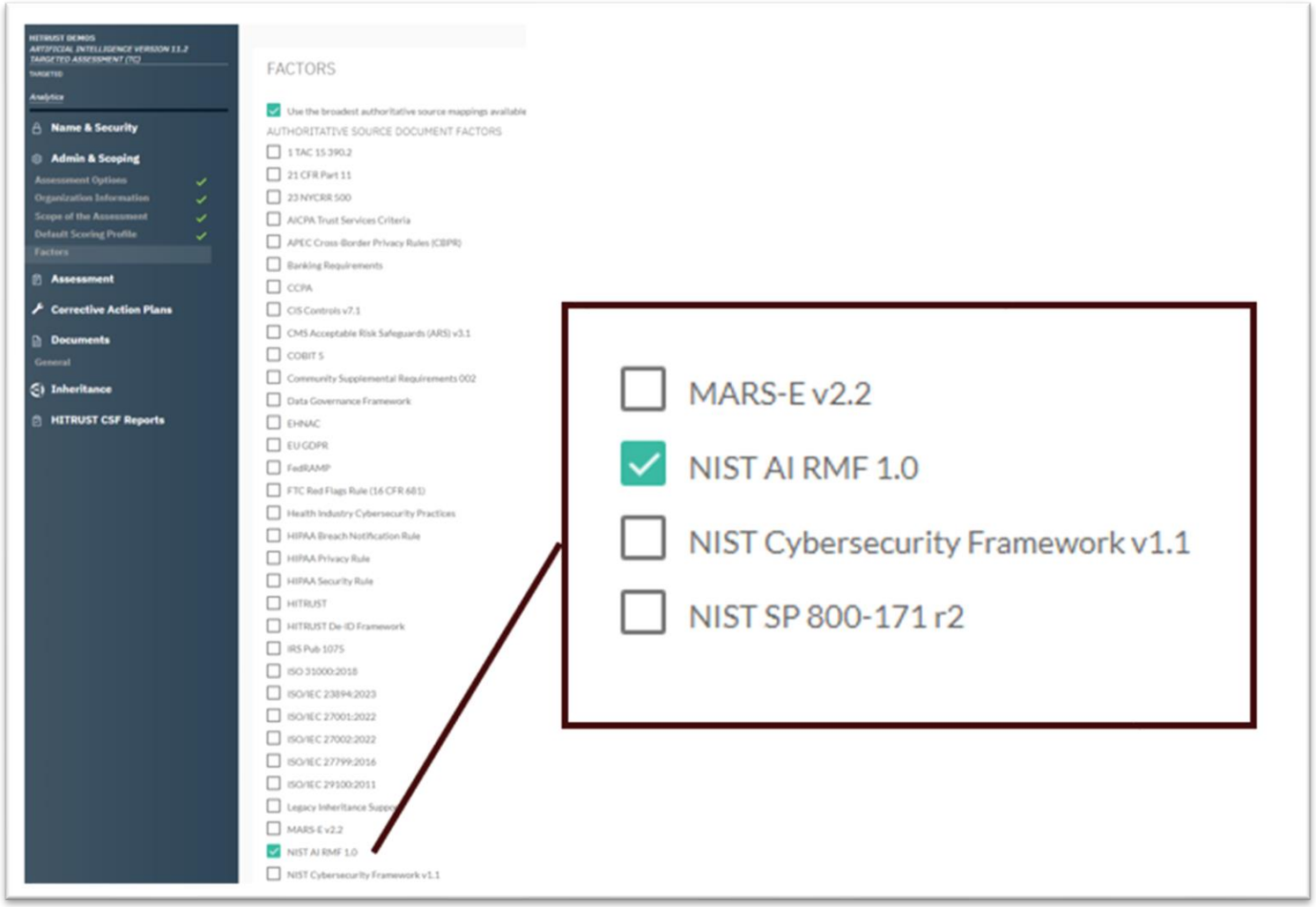
MyCSF – Generate a Targeted AI Assessment



Customers interested in only the AI controls from various frameworks can include them in a specially configured "Targeted, Current State (tC)" assessment. Configuration options shown here.

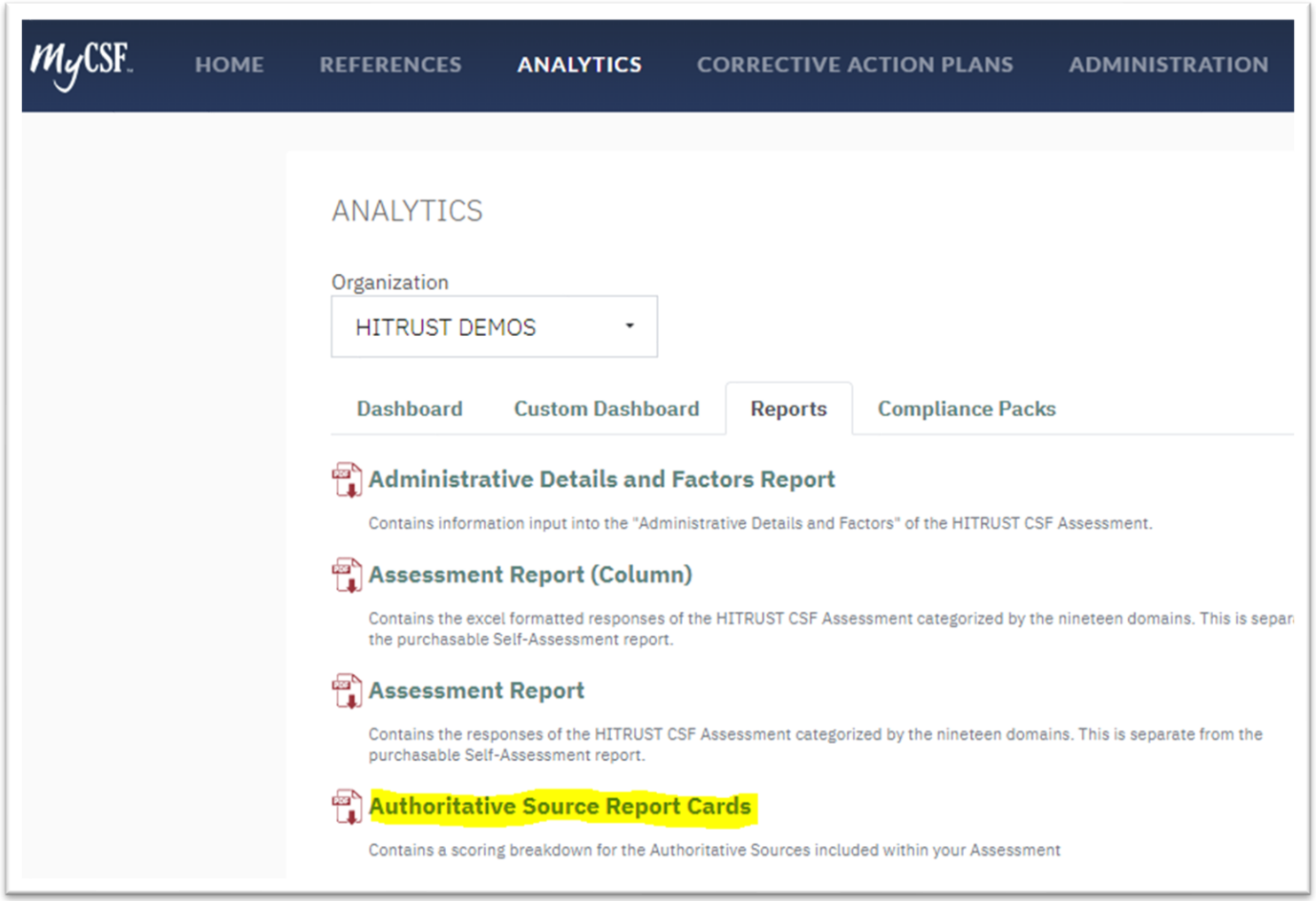
HITRUST

MyCSF – Generate a Targeted AI Assessment



Customers interested in only the AI controls from various frameworks can include them in a specially configured "Targeted, Current State (tC)" assessment. Configuration options shown here.

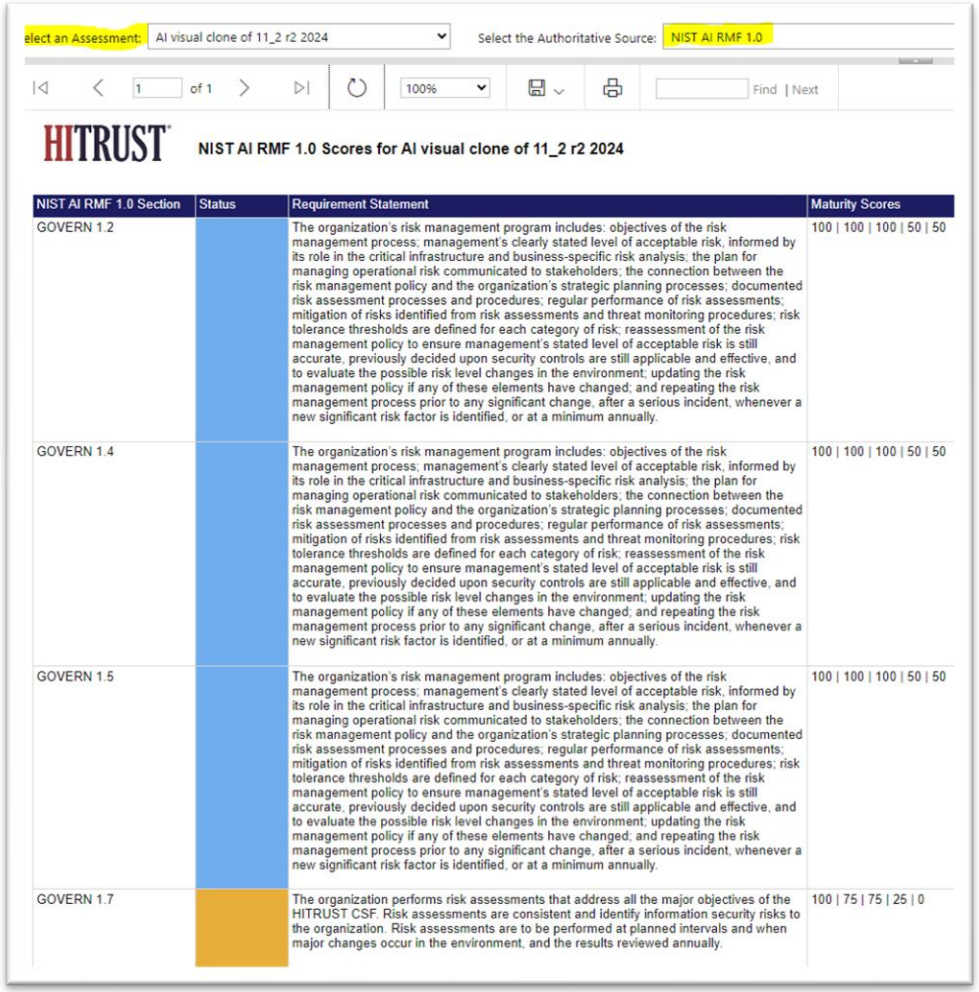
MyCSF – Generate an AI Scorecard



Customers completing a MyCSF assessment can see how they are performing relative to the AI controls included in the assessment. Navigate to "Analytics" and click on the "reports" tab as shown here. Select the "Authoritative Source Report Cards."

HITRUST

MyCSF – See Results with an AI Scorecard



elect an Assessment: AI visual clone of 11_2 r2 2024 Select the Authoritative Source: NIST AI RMF 1.0

1 of 1 100% Find | Next

HITRUST NIST AI RMF 1.0 Scores for AI visual clone of 11_2 r2 2024

NIST AI RMF 1.0 Section	Status	Requirement Statement	Maturity Scores
GOVERN 1.2		The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.	100 | 100 | 100 | 50 | 50
GOVERN 1.4		The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.	100 | 100 | 100 | 50 | 50
GOVERN 1.5		The organization's risk management program includes: objectives of the risk management process; management's clearly stated level of acceptable risk, informed by its role in the critical infrastructure and business-specific risk analysis; the plan for managing operational risk communicated to stakeholders; the connection between the risk management policy and the organization's strategic planning processes; documented risk assessment processes and procedures; regular performance of risk assessments; mitigation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk management policy to ensure management's stated level of acceptable risk is still accurate, previously decided upon security controls are still applicable and effective, and to evaluate the possible risk level changes in the environment; updating the risk management policy if any of these elements have changed; and repeating the risk management process prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.	100 | 100 | 100 | 50 | 50
GOVERN 1.7		The organization performs risk assessments that address all the major objectives of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization. Risk assessments are to be performed at planned intervals and when major changes occur in the environment, and the results reviewed annually.	100 | 75 | 75 | 25 | 0

Use the drop down menus to select your assessment containing the AI requirements, and then select the AI source "NIST AI RMF 1.0" or others. This will show completed scoring and status of those relevant AI requirement statements.

Thank you