

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

Authoritative Source	HITRUST Control Reference
GOVERN 1.1	03.a Risk Management Program Development
GOVERN 1.2	03.b Performing Risk Assessments
	03.a Risk Management Program Development
GOVERN 1.3	03.a Risk Management Program Development
GOVERN 1.4	03.c Risk Mitigation
	03.a Risk Management Program Development
GOVERN 1.5	00.a Information Security Management Program
	03.a Risk Management Program Development
GOVERN 1.6	07.a Inventory of Assets
	03.b Performing Rick Assessments
	03 a Rick Management Program Development
COVERN 1.7	01.h Redomine Bick Assessments
our est	03 a Eick Management Rougen Development
	At d Rick Fundamenters Program Generations
6.05.668.3.1	An a future star for the Management Bassan
00101423	All a Bick Management Research Considerated
COL858 3.3	10. a hijk Management Program Development
00118N 2.2	101.8 Kota Management Program Development
CONTRIN 2.3	VOLC MOR MERGADON
all days by	103.a Risk Management Program Development
GOVERN 3.1	103.a Risk Management Program Development
	03.b Performing Risk Assessments
GOVERN 3.2	03.c Risk Mitigation
	03.a Risk Management Program Development
	00.a Information Security Management Program
GOVERN 4.1	03.a Risk Management Program Development
GOVERN 4.2	03.a Risk Management Program Development
	03.b Performing Risk Assessments
GOVERN 4.3	03.a Risk Management Program Development
	03.b Performing Risk Assessments
	03.c Risk Mitigation
GOVERN 5.1	03.a Risk Management Program Development
GOVERN 5.2	03.a Risk Management Program Development
	03.b Performing Risk Assessments
GOVERN 6.1	03.a Risk Management Program evelopment
GOVERN 6.2	03 a Risk Management Program Development
	01 c Risk Mitigation
MANAGE 1.1	00 a Information Security Management Program
	01 a Bick Management Desalignment
	All a Bub Millioning
MANAGE 1.3	All a Rick Management Reserves Development
moved of \$14	13 b Business Councils and Rick Assessment
	12.0 Business Community and hisk Assessment
	DLC Risk Medication
	103.b Performing Risk Assessments
MANAGE 1.3	03.c Risk to gation
	03.a Rosk Planagement Program Development
MANAGE 1.4	03.b Partorning Risk Assessments
	03.a risk Management Program Development
MANAGE 2.1	03 Risk Management Program Development
MANAGE 2.2	A Risk Management Program Development
MANAGE 2.3	03.b Performing Risk Assessments
	03.a Risk Management Program Development
MANAGE 2.4	01.c Risk Mitigation

	52 53	MANAGE 2.4	03.a Risk Management Program Development 03.c Risk Mitigation
	51	MANAGE 2.3	03.b Performing Risk Assessments
	50	MANAGE 2.2	03.a Risk Management Program Development
	49	MANAGE 2.1	03.a Risk Management Program Development
/	48		03.a Risk Management Program Development
1	47	MANAGE 1.4	03.b Performing Risk Assessments
	46		03.a Risk Management Program Development
	45	MANAGE 1.3	03.c Risk Mitigation

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.



Using the CSF to Identify AI Controls

GOVERN 2.1	00.a Information Se	curity Management Program
7	03.a Risk Managem	nent Program Development
3 GOVERN 2.2	03.a Risk Managem	nent Program Development
Control Reference: 03.a R Control Specification: Factor Type: Topics: Level 1 Imp Level 1 Organizational Factors: Level 1 System Factors:	isk Management Program Development Organizations shall develop and maintain a risk management program to manage risk to an acceptable level. Organizational plementation Requirements	
Level 1 Regulatory Factors:	FISMA HITRUST De-ID Framework Texas Medical Records Privacy Act CMS Minimum Security Requirements (High) High Low Moderate	shown here.
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 stateholders; 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 bierance 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 policy if any of these elements have changed; and repeating the risk management policy and prior to any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.	- -

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

MyCSF.	HOME	REFERENCES	ANALYTICS	CORRECTIVE ACTIO	N PLANS AD	MINISTRATION	TASKS	VIEWS	TIME TRACKER	Q
Assessment C	Options Information	^		De-ID Framework		vil Code § 1798 81 5		EHN	IAC	
Scope of the A	Assessment			De ID Hanevork		11 COUC 3 17 70.01.3				
Default Scorin	ng Profile								170 D	
			Banking F	Requirements	FedR/	4MP		210	FR Part 11	
🖹 Assessm	ent		23 NYCR	R 500	GDPR			Dire	ctTrust	
01 - Informati	on Protection P	rogram								
02 - Endpoint	Protection		PDPA (Sir	ngapore)	ССРА			SCIE	DSA	
04 - Mobile De	Media Security									
05 - Wireless	Security		Data Cou	orpanco Framowork	Suppl	omontal Paguiromor	ato		umunity Supplemental Requirements 002	
06 - Configura	tion Manageme	ent	Data Gov	CHIANCE FLAMEWOLK		mental Requiremen	115		induity supplemental Requirements 002	
07 - Vulnerabi	ility Manageme	nt	_		_			_		
08 - Network I	Protection		MARS-E	/2.2	L ISO/IE	C 27001:2022		ISO/	/IEC 27002:2022	
09 - Transmiss	sion Protection									
10 - Password	l Management		VA Direct	ive 6500		HIP Moderate-plus S	Security Baselines	Artif	ficial Intelligence Risk Management	
11 - Access Co	ontrol				₩ v5.0					
12 - Audit Log	ging & Monitori	ng								
13 - Education Awarenes	n, Training and ss		ISO 3100	0:2018	Legac	y Inheritance Suppor	rt	HICI	p ^^	
14 - Third Part	ty Assurance									
15 - Incident M	Management		NIST SP 8	800-171 r2 ^^	HIPA/	1 ~ ~		NIST	r SP 800-53 R4 ^^	
16 - Business	Continuity & Di	saster								

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

MyCSF. HOME REFERENCES	ANALYTICS CORRECTIVE ACTION	PLANS ADMINISTRATION TASKS	VIEWS TIME TRACKER Q
Assessment Options Organization Information Scope of the Assessment	Data Governance Framework	Supplemental Requirements	Community Supplemental Requirements 002
Default Scoring Profile Factors	MARS-E v2.2	ISO/IEC 27001:2022	ISO/IEC 27002:2022
Assessment O1 - Information Protection Program	VA Directive 6500	NY OHIP Moderate-plus Security Baselines v5.0	Artificial Intelligence Risk Management
02 - Endpoint Protection 03 - Portable Media Security 04 - Mobile Device Security	ISO 31000:2018	Legacy Inheritance Support	HICP ^^
05 - Wireless Security 06 - Configuration Management 07 - Vulnerability Management	NIST SP 800-171 r2 ^^	HIPAA ^^	NIST SP 800-53 R4 ^^
08 - Network Protection 09 - Transmission Protection 10 - Password Management	NIST SP 800-53 R5 ^^	FedRAMP ^^	Ontario Personal Health Information Protection Act ^^
11 - Access Control 12 - Audit Logging & Monitoring 13 - Education, Training and			
Awareness 14 - Third Party Assurance 15 - Incident Management	REFRESH ASSESSMENT >	VIEW LOGS	PREVIEW CHANGES APPLICABLE CONTROLS PREVIEW PROFILE
16 - Business Continuity & Disaster		© 2024 HITRUST Services Corp. Pr	ivacy Policy

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

SUMMARIZED DIFFERENCES

The table below outlines the key differences to this assessment's Control Requirements and/or Illustrative Procedures resulting from the change(s) that you are previewing. Download the detailed comparison report to see the detailed list of differences. Click "Apply Changes" to apply the change that you are previewing.

Control Requirements Added		48
CANCEL	XML	DOWNLOAD DETAILED COMPARISON REPORT

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
01.03alSO23894Organizational.12	Assessment	Control Requirement Added	issues associated with the implementation of the AI system.
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

HITRUST DEMOS ARTIFICIAL INTELLIGENCE VERSION 11.2 TARGETED ASSESSMENT (TC) TARGETED Analytics	ASSESSMENT OPTIONS	
A Name & Security	Select a Preset (Optional)	
Admin & Scoping	11 VALIDATED R2 VALIDATED 11 READINESS R2 READINESS TARGETED E1 READINESS E1 VALIDATED	
Assessment Options 🗸		
Organization Information	Will this assessment be submitted to HITRUST for certification consideration?*	
Default Scoring Profile	No	~
Factors		
🖹 Assessment	Assessment Type *	
Corrective Action Plans	Current state assessment targeted to specific authoritative sources (tC)	~
Documents General Inheritance HITRUST CSF Reports	CSF Version v11.2.0 Create Until: 10/29/2025 Submit By: Selected HITRUST CSF Assessment: Targeted Assessment (tC Readiness)	~
	SAVE & CONTINUE >	

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 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 Al Scorecard

MyCSF.	НОМЕ	REFERENCES	ANALYTICS	CORRECTIVE	ACTION PLANS	ADMINISTRATION
		ANALYTICS Organization HITRUST DEM Dashboard Contains informate Contains the exce the purchasable Self- Contains the resp purchasable Self- Contains the resp Contains the resp	IOS Custom Dashboa ive Details and ion input into the "Adm ion input into the "Adm icelf-Assessment report. Report Report Column ielf-Assessment report. Report onses of the HITRUST O Assessment report. Conses of the HITRUST O Conses of the HITRUST	Ird Reports Factors Report inistrative Details and Factors Report inistrative Details and Factors (a) of the HITRUST CSF Asso (SF Assessment categor) to Cards horitative Sources inclu	Compliance Packs actors" of the HITRUST CSF essment categorized by the rized by the nineteen domai	s Assessment. e nineteen domains. This is sepan ins. This is separate from the

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

HITRI

MyCSF – See Results with an AI Scorecard

⊲ < 1	of 1 >	⊳I	C	100%	~		₿	Find N	ext
HITRUST	NISTAIR	WF 1.0 Sc	ores 1	or Al visua	al clone	e of 11_2 r	2 2024		
IST AI RMF 1.0 Sectio	n Status	Require	ment St	atement					Maturity Scores
GOVERN 1.2		The org manage its role i managin risk mar risk ass mitigatio tolerano manage accurate to evalu manage new sig	The organization's risk management program includes: objectives of the risk management process: management program includes: objectives of the risk is role in the critical infrastructure and business-specific risk analysis: the plan for managing operational risk communicated to stakeholders; the connection between the isk 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 loterance 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 and 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 dentified, or at a minimum amunally.						
SOVERN 1.4		The org manage its role i managin risk mar risk ass mitigatic tolerance manage accuratic to evalu manage new sig	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; miligation of risks identified from risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the 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 of uses graphicate change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.						100 100 100 50 5
IOVERN 1.5		The org manage its role i managin risk mar risk ass mitigatio toleranc manage accurate to evalu manage manage new sig	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 assessments and procedures; regular performance of risk assessments; mitigation of risks is and effect form risk assessments and threat monitoring procedures; risk tolerance thresholds are defined for each category of risk; reassessment of the risk is all 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 polics; or any significant change, after a serious incident, whenever a new significant risk factor is identified, or at a minimum annually.						
GOVERN 1.7		The org HITRUS the orga	anizatio ST CSF. anization	n performs ri Risk assess n. Risk asses	sk asses ments ar sments a	sments that a consistent of the perf	address all and identif ormed at p	the major objectives of the y information security risks to lanned intervals and when	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