



v11.4.0 Summary of Changes

Difference Comparison for
CSF v11.3.0 to v11.4.0

HITRUST[®]

Table of Contents

CSF Library Version.....	3
CSF Control Objective.....	4
CSF Question Requirement Record.....	5
Authoritative Source Document.....	43
Factor Type.....	46
Factor.....	70

Changes for Library Version View D T O - v11.3.0 to v11.4.0

Library Version View D T O: v11.4.0

Change Count: 1

Field	Content
Name	v11. ~~33~~ ⁴ 4.0

Changes for Control Objective View D T O - v11.3.0 to v11.4.0

Control Objective View D T O: CSFControlObjectiveViewDTO { Id = 7310, CurrentlyWithUserId = michael.moore@hitrustalliance.net, ApprovalWorkflowInstanceId = 57d811aa93b9442882a729bfba3d950f, SubmitterId = jeremy.huval@hitrustalliance.net, SubmitterComments = fixed html tag at end, ApprovalWorkflowInitiatedOn = 11/22/2024 20:49:18, PeerReviewerId = , PeerReviewerComments = , PeerReviewedOn = , VPRReviewerId = , VPRReviewerComments = , VPRReviewedOn = , QARReviewerId = michael.moore@hitrustalliance.net, QARReviewerComments = , QARReviewedOn = , Level = Completed, CreatedBy = andrew.russell@hitrustalliance.net, CreatedOn = 04/16/2024 13:36:18, ModifiedBy = jeremy.huval@hitrustalliance.net, ModifiedOn = 11/22/2024 20:49:18, ChangeNarrative = Approval workflow initiated, LineageId = 6967, CSFControlCategoryId = 2135, Name = 10.06 Technical Vulnerability Management, Description = <body style="font-family: Arial;"><p>To reduce the risks resulting from exploitation of published technical vulnerabilities, technical vulnerability management shall be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.</p> </body>, CSFControlReferences = }

Change Count: 1

Field	Content
Description	To reduce the risks resulting from exploitation of published technical vulnerabilities, technical vulnerability management shall be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness.

Changes for Question Requirement Record - v11.3.0 to v11.4.0

Question Requirement Record: 19.06bOWASPOrganizational.1 / 2994.0

Change Count: 0

Field	Content
New Question Requirement Record	19.06bOWASPOrganizational.1 / 2994.0

Question Requirement Record: 06.10hAISecSystem.4 / 3078.0

Change Count: 0

Field	Content
New Question Requirement Record	06.10hAISecSystem.4 / 3078.0

Question Requirement Record: 06.10hAISecSystem.7 / 3077.0

Change Count: 0

Field	Content
New Question Requirement Record	06.10hAISecSystem.7 / 3077.0

Question Requirement Record: 07.10mStateRAMPOrganizational.2 / 3076.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10mStateRAMPOrganizational.2 / 3076.0

Question Requirement Record: 11.01qStateRAMPSystem.1 / 3075.0

Change Count: 0

Field	Content
New Question Requirement Record	11.01qStateRAMPSystem.1 / 3075.0

Question Requirement Record: 12.09hStateRAMPSystem.1 / 3074.0

Change Count: 0

Field	Content
New Question Requirement Record	12.09hStateRAMPSystem.1 / 3074.0

Question Requirement Record: 11.01bStateRAMPSystem.2 / 3073.0

Change Count: 0

Field	Content
New Question Requirement Record	11.01bStateRAMPSystem.2 / 3073.0

Question Requirement Record: 07.10mStateRAMPOrganizational.1 / 3072.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	07.10mStateRAMPOrganizational.1 / 3072.0
---------------------------------	--

Question Requirement Record: 12.09abStateRAMPSystem.1 / 3071.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	12.09abStateRAMPSystem.1 / 3071.0
---------------------------------	-----------------------------------

Question Requirement Record: 11.01bStateRAMPSystem.1 / 3070.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	11.01bStateRAMPSystem.1 / 3070.0
---------------------------------	----------------------------------

Question Requirement Record: 07.10mAIISecOrganizational.3 / 3042.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	07.10mAIISecOrganizational.3 / 3042.0
---------------------------------	---------------------------------------

Question Requirement Record: 16.09IAISecOrganizational.1 / 3067.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	16.09IAISecOrganizational.1 / 3067.0
---------------------------------	--------------------------------------

Question Requirement Record: 15.11cAIISecOrganizational.1 / 3069.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	15.11cAIISecOrganizational.1 / 3069.0
---------------------------------	---------------------------------------

Question Requirement Record: 07.10eAIISecSystem.1 / 3068.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	07.10eAIISecSystem.1 / 3068.0
---------------------------------	-------------------------------

Question Requirement Record: 07.07aAI SecOrganizational.5 / 3066.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	07.07aAI SecOrganizational.5 / 3066.0
---------------------------------	---------------------------------------

Question Requirement Record: 07.07aAI SecOrganizational.4 / 3065.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	07.07aAI SecOrganizational.4 / 3065.0
---------------------------------	---------------------------------------

Question Requirement Record: 07.07aAI SecOrganizational.3 / 3064.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	07.07aAI SecOrganizational.3 / 3064.0
---------------------------------	---------------------------------------

Question Requirement Record: 12.09abAI SecSystem.5 / 3063.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	12.09abAI SecSystem.5 / 3063.0
---------------------------------	--------------------------------

Question Requirement Record: 12.09abAI SecSystem.4 / 3062.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	12.09abAI SecSystem.4 / 3062.0
---------------------------------	--------------------------------

Question Requirement Record: 11.01vAI SecSystem.1 / 3060.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	11.01vAI SecSystem.1 / 3060.0
---------------------------------	-------------------------------

Question Requirement Record: 11.01cAI SecSystem.9 / 3058.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	11.01cAI SecSystem.9 / 3058.0
---------------------------------	-------------------------------

Question Requirement Record: 11.01cAISecSystem.8 / 3057.0

Change Count: 0

Field	Content
New Question Requirement Record	11.01cAISecSystem.8 / 3057.0

Question Requirement Record: 11.01cAISecSystem.7 / 3056.0

Change Count: 0

Field	Content
New Question Requirement Record	11.01cAISecSystem.7 / 3056.0

Question Requirement Record: 11.01cAISecSystem.6 / 3055.0

Change Count: 0

Field	Content
New Question Requirement Record	11.01cAISecSystem.6 / 3055.0

Question Requirement Record: 11.01cAISecSystem.5 / 3054.0

Change Count: 0

Field	Content
New Question Requirement Record	11.01cAISecSystem.5 / 3054.0

Question Requirement Record: 17.03bAISecOrganizational.3 / 3052.0

Change Count: 0

Field	Content
New Question Requirement Record	17.03bAISecOrganizational.3 / 3052.0

Question Requirement Record: 14.05kAISecOrganizational.1 / 3051.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05kAISecOrganizational.1 / 3051.0

Question Requirement Record: 14.05iAISecOrganizational.1 / 3050.0

Change Count: 0

Field	Content
New Question Requirement Record	14.05iAISecOrganizational.1 / 3050.0

Question Requirement Record: 14.09fAI SecSystem.1 / 3049.0

Change Count: 0

Field

Content

New Question Requirement Record

14.09fAI SecSystem.1 / 3049.0

Question Requirement Record: 07.10mAI SecOrganizational.2 / 3048.0

Change Count: 0

Field

Content

New Question Requirement Record

07.10mAI SecOrganizational.2 / 3048.0

Question Requirement Record: 19.06cAI SecOrganizational.1 / 3046.0

Change Count: 0

Field

Content

New Question Requirement Record

19.06cAI SecOrganizational.1 / 3046.0

Question Requirement Record: 06.10hAI SecSystem.6 / 3045.0

Change Count: 0

Field

Content

New Question Requirement Record

06.10hAI SecSystem.6 / 3045.0

Question Requirement Record: 06.10hAI SecSystem.5 / 3044.0

Change Count: 0

Field

Content

New Question Requirement Record

06.10hAI SecSystem.5 / 3044.0

Question Requirement Record: 06.09bAI SecSystem.1 / 3043.0

Change Count: 0

Field

Content

New Question Requirement Record

06.09bAI SecSystem.1 / 3043.0

Question Requirement Record: 06.10jAI SecSystem.1 / 3041.0

Change Count: 0

Field

Content

New Question Requirement Record

06.10jAI SecSystem.1 / 3041.0

Question Requirement Record: 13.02eAISecOrganizational.1 / 3040.0

Change Count: 0

Field	Content
New Question Requirement Record	13.02eAISecOrganizational.1 / 3040.0

Question Requirement Record: 12.09abAISecSystem.3 / 3039.0

Change Count: 0

Field	Content
New Question Requirement Record	12.09abAISecSystem.3 / 3039.0

Question Requirement Record: 01.00aAISecOrganizational.1 / 3038.0

Change Count: 0

Field	Content
New Question Requirement Record	01.00aAISecOrganizational.1 / 3038.0

Question Requirement Record: 01.02aAISecOrganizational.1 / 3037.0

Change Count: 0

Field	Content
New Question Requirement Record	01.02aAISecOrganizational.1 / 3037.0

Question Requirement Record: 07.06hAISecOrganizational.1 / 3036.0

Change Count: 0

Field	Content
New Question Requirement Record	07.06hAISecOrganizational.1 / 3036.0

Question Requirement Record: 17.03bAISecOrganizational.5 / 3035.0

Change Count: 0

Field	Content
New Question Requirement Record	17.03bAISecOrganizational.5 / 3035.0

Question Requirement Record: 17.03bAISecOrganizational.4 / 3034.0

Change Count: 0

Field	Content
New Question Requirement Record	17.03bAISecOrganizational.4 / 3034.0

Question Requirement Record: 15.09tDORAOrganizational.2 / 3033.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	15.09tDORAOrganizational.2 / 3033.0
---------------------------------	-------------------------------------

Question Requirement Record: 17.03aDORAOrganizational.1 / 3032.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	17.03aDORAOrganizational.1 / 3032.0
---------------------------------	-------------------------------------

Question Requirement Record: 14.05iDORAOrganizational.2 / 3031.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	14.05iDORAOrganizational.2 / 3031.0
---------------------------------	-------------------------------------

Question Requirement Record: 17.03dDORAOrganizational.2 / 3030.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	17.03dDORAOrganizational.2 / 3030.0
---------------------------------	-------------------------------------

Question Requirement Record: 07.10mDORAOrganizational.2 / 3029.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	07.10mDORAOrganizational.2 / 3029.0
---------------------------------	-------------------------------------

Question Requirement Record: 15.09tDORAOrganizational.1 / 3028.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	15.09tDORAOrganizational.1 / 3028.0
---------------------------------	-------------------------------------

Question Requirement Record: 14.09eDORASystem.1 / 3027.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	14.09eDORASystem.1 / 3027.0
---------------------------------	-----------------------------

Question Requirement Record: 14.05kDORAOrganizational.7 / 3026.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	14.05kDORAOrganizational.7 / 3026.0
---------------------------------	-------------------------------------

Question Requirement Record: 14.05iDORAOrganizational.1 / 3025.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	14.05iDORAOrganizational.1 / 3025.0
---------------------------------	-------------------------------------

Question Requirement Record: 14.05kDORAOrganizational.6 / 3024.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	14.05kDORAOrganizational.6 / 3024.0
---------------------------------	-------------------------------------

Question Requirement Record: 14.05kDORAOrganizational.5 / 3023.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	14.05kDORAOrganizational.5 / 3023.0
---------------------------------	-------------------------------------

Question Requirement Record: 14.05kDORAOrganizational.4 / 3022.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	14.05kDORAOrganizational.4 / 3022.0
---------------------------------	-------------------------------------

Question Requirement Record: 14.05kDORAOrganizational.3 / 3021.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	14.05kDORAOrganizational.3 / 3021.0
---------------------------------	-------------------------------------

Question Requirement Record: 14.05kDORAOrganizational.2 / 3020.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	14.05kDORAOrganizational.2 / 3020.0
---------------------------------	-------------------------------------

Question Requirement Record: 14.05kDORAOrganizational.1 / 3019.0

Change Count: 0

Field

Content

New Question Requirement Record	14.05kDORAOrganizational.1 / 3019.0
---------------------------------	-------------------------------------

Question Requirement Record: 07.10mDORAOrganizational.1 / 3018.0

Change Count: 0

Field

Content

New Question Requirement Record	07.10mDORAOrganizational.1 / 3018.0
---------------------------------	-------------------------------------

Question Requirement Record: 17.03dDORAOrganizational.1 / 3017.0

Change Count: 0

Field

Content

New Question Requirement Record	17.03dDORAOrganizational.1 / 3017.0
---------------------------------	-------------------------------------

Question Requirement Record: 17.11aDORAOrganizational.1 / 3016.0

Change Count: 0

Field

Content

New Question Requirement Record	17.11aDORAOrganizational.1 / 3016.0
---------------------------------	-------------------------------------

Question Requirement Record: 16.12eDORAOrganizational.1 / 3015.0

Change Count: 0

Field

Content

New Question Requirement Record	16.12eDORAOrganizational.1 / 3015.0
---------------------------------	-------------------------------------

Question Requirement Record: 15.11aNAIC668Organizational.3 / 3014.0

Change Count: 0

Field

Content

New Question Requirement Record	15.11aNAIC668Organizational.3 / 3014.0
---------------------------------	--

Question Requirement Record: 15.11aNAIC668Organizational.2 / 3013.0

Change Count: 0

Field

Content

New Question Requirement Record	15.11aNAIC668Organizational.2 / 3013.0
---------------------------------	--

Question Requirement Record: 15.11aNAIC668Organizational.1 / 3012.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	15.11aNAIC668Organizational.1 / 3012.0
---------------------------------	--

Question Requirement Record: 01.00aNAIC668Organizational.1 / 3011.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	01.00aNAIC668Organizational.1 / 3011.0
---------------------------------	--

Question Requirement Record: 16.12cCMSOrganizational.13 / 3010.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	16.12cCMSOrganizational.13 / 3010.0
---------------------------------	-------------------------------------

Question Requirement Record: 16.12cCMSOrganizational.12 / 3009.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	16.12cCMSOrganizational.12 / 3009.0
---------------------------------	-------------------------------------

Question Requirement Record: 19.13aCMSOrganizational.1 / 3008.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	19.13aCMSOrganizational.1 / 3008.0
---------------------------------	------------------------------------

Question Requirement Record: 10.01dCMSSystem.9 / 3007.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	10.01dCMSSystem.9 / 3007.0
---------------------------------	----------------------------

Question Requirement Record: 16.09ICMSOrganizational.5 / 3006.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	16.09ICMSOrganizational.5 / 3006.0
---------------------------------	------------------------------------

Question Requirement Record: 19.13qCMSOrganizational.2 / 3005.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record

19.13qCMSOrganizational.2 / 3005.0

Question Requirement Record: 11.01bCMSSystem.6 / 3004.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record

11.01bCMSSystem.6 / 3004.0

Question Requirement Record: 11.01bCMSSystem.4 / 3003.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record

11.01bCMSSystem.4 / 3003.0

Question Requirement Record: 19.13IGLBAOrganizational.1 / 3002.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record

19.13IGLBAOrganizational.1 / 3002.0

Question Requirement Record: 09.09sAISecOrganizational.1 / 3000.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record

09.09sAISecOrganizational.1 / 3000.0

Question Requirement Record: 19.10eOWASPSSystem.2 / 2999.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record

19.10eOWASPSSystem.2 / 2999.0

Question Requirement Record: 12.09acOWASPSSystem.1 / 2998.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record

12.09acOWASPSSystem.1 / 2998.0

Question Requirement Record: 06.09dOWASPSystem.1 / 2997.0

Change Count: 0

Field	Content
New Question Requirement Record	06.09dOWASPSystem.1 / 2997.0

Question Requirement Record: 07.09jOWASPOrganizational.1 / 2996.0

Change Count: 0

Field	Content
New Question Requirement Record	07.09jOWASPOrganizational.1 / 2996.0

Question Requirement Record: 06.10jOWASPSystem.3 / 2995.0

Change Count: 0

Field	Content
New Question Requirement Record	06.10jOWASPSystem.3 / 2995.0

Question Requirement Record: 06.10jOWASPSystem.1 / 2993.0

Change Count: 0

Field	Content
New Question Requirement Record	06.10jOWASPSystem.1 / 2993.0

Question Requirement Record: 07.10mOWASPOrganizational.10 / 2992.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10mOWASPOrganizational.10 / 2992.0

Question Requirement Record: 07.10mOWASPOrganizational.7 / 2988.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10mOWASPOrganizational.7 / 2988.0

Question Requirement Record: 07.10mOWASPOrganizational.6 / 2987.0

Change Count: 0

Field	Content
New Question Requirement Record	07.10mOWASPOrganizational.6 / 2987.0

Question Requirement Record: 19.13aTMRPAOrganizational.1 / 2986.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	19.13aTMRPAOrganizational.1 / 2986.0
---------------------------------	--------------------------------------

Question Requirement Record: 19.13fTMRPAOrganizational.3 / 2985.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	19.13fTMRPAOrganizational.3 / 2985.0
---------------------------------	--------------------------------------

Question Requirement Record: 19.13fTMRPAOrganizational.2 / 2984.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	19.13fTMRPAOrganizational.2 / 2984.0
---------------------------------	--------------------------------------

Question Requirement Record: 19.09qTMRPAOrganizational.1 / 2983.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	19.09qTMRPAOrganizational.1 / 2983.0
---------------------------------	--------------------------------------

Question Requirement Record: 19.13dTMRPAOrganizational.2 / 2982.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	19.13dTMRPAOrganizational.2 / 2982.0
---------------------------------	--------------------------------------

Question Requirement Record: 19.13dTMRPAOrganizational.1 / 2981.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	19.13dTMRPAOrganizational.1 / 2981.0
---------------------------------	--------------------------------------

Question Requirement Record: 19.13fTMRPAOrganizational.1 / 2980.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	19.13fTMRPAOrganizational.1 / 2980.0
---------------------------------	--------------------------------------

Question Requirement Record: 13.02eTMRPAOrganizational.3 / 2979.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	13.02eTMRPAOrganizational.3 / 2979.0
---------------------------------	--------------------------------------

Question Requirement Record: 13.02eTMRPAOrganizational.2 / 2978.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	13.02eTMRPAOrganizational.2 / 2978.0
---------------------------------	--------------------------------------

Question Requirement Record: 13.02eTMRPAOrganizational.1 / 2977.0

Change Count: 0

Field	Content
-------	---------

New Question Requirement Record	13.02eTMRPAOrganizational.1 / 2977.0
---------------------------------	--------------------------------------

Question Requirement Record: 06.09abNIST80053System.9 / 1887.0

Change Count: 1

Field	Content
-------	---------

BaselineUniqueld	06.06h6h9ab9abNIST80053Organizational.2Organizational.2 System.9System.9
------------------	---

Question Requirement Record: 02.09jTXRAMPOrganizational.2 / 0878.0

Change Count: 1

Field	Content
-------	---------

RequirementStatement	Malicious code is blocked and quarantined. An alert is sent to administrators in response to in response to upon upon detection.
----------------------	--

Question Requirement Record: 12.09abFFIECCATSystem.5 / 2899.0

Change Count: 1

Field	Content
-------	---------

IllustrativeProcedureMeasured	For example, measures indicate the number of alerts generated from fictitious confidential data or files being accessed. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to verify the organization uses tags on fictitious confidential data or files to provide advanced alerts of potential malicious activity when the data is accessed.
-------------------------------	---

Change Count: 5

Field	Content
BaselineUniqueld	19.06aOWASPOWASP AI SecAISecOrganizational.2211
CrossVersionId	2957.0011
RequirementStatement	The organization <i>checks laws and regulations</i> checks laws and regulations performs an assessment to identify and evaluate its compliance with applicable legal and performs an assessment to identify and evaluate its compliance with applicable legal and regu <i>gulated toed to</i> ory requirements addressing ory requirements addressing the development and <i>use</i> used deployment deployment of AI systems <i>on a recurring basis in order to validate the compliance of the AI system</i> on a recurring basis in order to validate the compliance of the AI system, including potential liability for harmful, infringing, or damaging outputs or behaviors. This assessment is performed prior to deployment of the AI system, and regularly (at least annually) thereafter, including potential liability for harmful, infringing, or damaging outputs or behaviors. This assessment is performed prior to deployment of the AI system, and regularly (at least annually) thereafter.
IllustrativeProcedureImplemented	For example, <i>obtain and examine evidence to confirm that</i> obtain and examine evidence to confirm that review the organizations assessment documentation to evaluate its compliance with review the organizations assessment documentation to evaluate its compliance with applicable <i>laws</i> awsega legal and regulations <i>related to</i> ions related to ory requirements addressing ory requirements addressing the development and <i>use</i> used deployment deployment of AI systems <i>were checked on a recurring basis</i> were checked on a recurring basis, including potential liability for harmful, infringing, or damaging outputs or behaviors. Further, confirm that an assessment is performed prior to deployment of the AI system (if within the past year), and regularly (at least annually) thereafter, including potential liability for harmful, infringing, or damaging outputs or behaviors. Further, confirm that an assessment is performed prior to deployment of the AI system (if within the past year), and regularly (at least annually) thereafter.

IllustrativeProcedureMeasured	For example, measures indicate <i>the percentage of</i> the percentage of completeness of the organization's assessment to identify and evaluate its compliance with completeness of the organization's assessment to identify and evaluate its compliance with applicable <i>laws</i> legal and regulations related to <i>ions related to</i> ory requirements addressing <i>ory requirements</i> addressing the development and <i>use</i> deployment deployment of AI systems <i>that are checked on a recurring basis</i> that are checked on a recurring basis. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the <i>e applicable laws and regulations related to the</i> applicable laws and regulations related to the at an assessment is performed prior to at an assessment is performed prior to <i>deve</i> pploppyment and use of and use of <i>of the</i> of the AI systems <i>ss,, are checked on a recurring basis in order to validate the compliance of the AI sys</i> re checked on a recurring basis in order to validate the compliance of the AI sys nd regularly (at least annually) thereaf nd regularly (at least annually) thereafter <i>mrrr</i>.
-------------------------------	--

Question Requirement Record: 12.09abAISecSystem.6 / 2971.1

Change Count: 5

Field	Content
BaselineUniqueld	12.09abOWASPOWASP AI SecAISecSystem.2266
CrossVersionId	2971.0011
RequirementStatement	<i>AI model usage is logged. AI model usage logs are incorporated into the organization's incident detection capability</i> AI model usage is logged. AI model usage logs are incorporated into the organization's incident detection capability The AI system logs all inputs (prompts, queries, inference requests) to and outputs (inferences, responses, conclusions) from the AI model, including the exact input (e.g., the prompt, the API call), the date and time of the input, the user account making the request, where the request originated, the exact output provided, and the version of the model used. AI system logs are managed (i.e., retained, protected, and sanitized) in accordance with the organization's policy requirements The AI system logs all inputs (prompts, queries, inference requests) to and outputs (inferences, responses, conclusions) from the AI model, including the exact input (e.g., the prompt, the API call), the date and time of the input, the user account making the request, where the request originated, the exact output provided, and the version of the model used. AI system logs are managed (i.e., retained, protected, and sanitized) in accordance with the organization's policy requirements.

IllustrativeProcedureImplemented	For example, <i>select a sample of AI model usage logs and examine evidence they</i>select a sample of AI model usage logs and examine evidence they<i>review the AI system to ensure the organization logs all inputs (prompts, queries, inference requests) to and outputs (inferences, responses, conclusions) from the AI model, including the exact input, the date and time of the input, the user account making the request,</i>review the AI system to ensure the organization logs all inputs (prompts, queries, inference requests) to and outputs (inferences, responses, conclusions) from the AI model, including the exact input, the date and time of the input, the user account making the request, <i>wh</i>here <i>incorporated into the organization's incident detection capability</i>incorporated into the organization's incident detection capability<i>the request originated, the exact output provided, and the version of the model used. Further, confirm the AI system logs are managed (i.e., retained, protected, and sanitized) in accordance with the organization's policy requirements</i>the request originated, the exact output provided, and the version of the model used. Further, confirm the AI system logs are managed (i.e., retained, protected, and sanitized) in accordance with the organization's policy requirements.
IllustrativeProcedureMeasured	For example, measures indicate <i>if</i> if the <i>number of AI model related incidents detected by the organization's incident detection capability</i>number of AI model related incidents detected by the organization's incident detection capability<i>organization logs all inputs (prompts, queries, inference requests) to and outputs (inferences, responses, conclusions) from the AI model, including the exact input, the date and time of the input, the user account making the request, where the request originated, the exact output provided, and the version of the model used</i>organization logs all inputs (prompts, queries, inference requests) to and outputs (inferences, responses, conclusions) from the AI model, including the exact input, the date and time of the input, the user account making the request, where the request originated, the exact output provided, and the version of the model used. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm <i>AI model usage is logged and AI model usage logs are incorporated into</i>AI model usage is logged and AI model usage logs are incorporated into<i>the AI system logs are managed (i.e., retained, protected, and sanitized) in accordance with</i>the AI system logs are managed (i.e., retained, protected, and sanitized) in accordance with the organization's <i>incident detection capability</i>incident detection capability<i>policy requirements</i>policy requirements.

Question Requirement Record: 07.10mAI SecOrganizational.4 / 2913.0

Change Count: 1

Field	Content
BaselineUniqueld	07.10mOWASPOWASP AI SecAI SecOrganizational. 5544

Question Requirement Record: 07.10mOWASPOrganizational.3 / 2965.0

Change Count: 4

Field	Content
RequirementStatement	The organization adds adversarial examples to <i>the</i> the AI training data to make the model more resilient to attacks to attacks.
IllustrativeProcedureImplemented	For example, <i>obtain and examine evidence to confirm the addition of adversarial examples to the AI training data</i> obtain and examine evidence to confirm the addition of adversarial examples to the AI training data select a sample of the organizations AI training data to confirm it includes adversarial examples to make the model more resilient to attacks select a sample of the organizations AI training data to confirm it includes adversarial examples to make the model more resilient to attacks.
IllustrativeProcedureMeasured	For example, measures indicate if if the <i>volume of adversarial examples as a percentage of all AI training data</i> volume of adversarial examples as a percentage of all AI training data organizations AI training data includes adversarial examples organizations AI training data includes adversarial examples. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm <i>the addition of adversarial examples to the AI training data</i> addition of adversarial examples to the AI training data at all AI training data includes adversarial examples to make the model more resilient to attacks at all AI training data includes adversarial examples to make the model more resilient to attacks.
DITA	Sampling Sampling

Question Requirement Record: 19.13jAISecOrganizational.1 / 2958.0

Change Count: 4

Field	Content
BaselineUniqueld	19.13jOWASPOWASP AISec AISecOrganizational.1
RequirementStatement	The organization <i>removes or anonymizes</i> moves or anonymizes views the data used to train AI models, fine-tune AI models, and enhance AI prompts via RAG to identify any views the data used to train AI models, fine-tune AI models, and enhance AI prompts via RAG to identify any data fields or records that <i>are not needed</i> are not need can be omitted can be omitted <i>for the AI system (e.g., in AI training data), to prevent them from leaking</i> the AI system (e.g., in AI training data), to prevent them from leaking anonymized (to prevent them from potentially leaking) and takes action on findings anonymized (to prevent them from potentially leaking) and takes action on findings.

IllustrativeProcedureImplemented	For example, <i>obtain and examine evidence to confirm data fields or records that are not needed for the AI system (e.g., in AI training data) were removed or anonymized</i> obtain and examine evidence to confirm data fields or records that are not needed for the AI system (e.g., in AI training data) were removed or anonymized evaluate the AI model to ensure the organization reviews the data used to train AI models, fine-tune AI models, and enhance AI prompts via RAG to identify any data fields or records that can be omitted or anonymized (to prevent them from potentially leaking) and takes action on findings evaluate the AI model to ensure the organization reviews the data used to train AI models, fine-tune AI models, and enhance AI prompts via RAG to identify any data fields or records that can be omitted or anonymized (to prevent them from potentially leaking) and takes action on findings.
IllustrativeProcedureMeasured	For example, measures indicate the <i>number of records removed or anonymized. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that all data fields or records that are not needed for the AI system are removed or anonymized</i> number of records removed or anonymized. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that all data fields or records that are not needed for the AI system are removed or anonymized percentage of the organization's AI datasets which have undergone this review percentage of the organization's AI datasets which have undergone this review.

Question Requirement Record: 06.10cATLASSystem.1 / 2954.0

Change Count: 2

Field	Content
RequirementStatement	The organization establishes a content policy that defines unwanted content (e.g., explicit or eeo offensive language), removes unwanted content from data used to train machine learning models, and implements a filter to limit ingested training data based on this content policy.
IllustrativeProcedureMeasured	For example, measures indicate the existence of unwanted content within the machine learning training data. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization establishes a content policy that defines unwanted content (e.g., explicit or eeo offensive language), removes unwanted content from data used to train machine learning models, and implements a filter to limit ingested training data based on this content policy.

Question Requirement Record: 07.09mNIST800172Organizational.2 / 2930.0

Change Count: 1

Field	Content
BaselineUniqueld	07.07a7a9m9mNIST800172Organizational.1122

Change Count: 4

Field	Content
BaselineUniqueld	07.10bA ~~TL~~ AS ~~TL~~ ASISecISecSystem.4411
RequirementStatement	<i>The information system p</i>Before they <i>a</i>Before they are processes <i>all model inputs before they reach</i> <i>the production machine learning model to nullify or reverse</i> <i>potential adversarial perturbations</i>s all model inputs before they reach the production machine learning model to nullify or reverse potential adversarial perturbationsd by the model, the AI system actively filters user inputs (regardless of modality or source, including attachments) for suspicious and/or unexpected values or patterns which could be adversarial or malicious in natured by the model, the AI system actively filters user inputs (regardless of modality or source, including attachments) for suspicious and/or unexpected values or patterns which could be adversarial or malicious in nature.
IllustrativeProcedureImplemented	For example, <i>obtain and examine evidence to confirm the</i> <i>system preprocessed all model inputs</i>obtain and examine evidence to confirm the system preprocessed all model inputs review the AI system configurations to ensure that user inputs (regardless of modality or source, including attachments) are actively filteredreview the AI system configurations to ensure that user inputs (regardless of modality or source, including attachments) are actively filtered before they reached the <i>production machine learning</i> production machine learning model.

IllustrativeProcedureMeasured	For example, measures indicate if if the <i>percentage of model inputs which were not preprocessed before reaching the production machine learning model. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the information system preprocesses all model inputs before they reach the production machine learning model to nullify or reverse potential adversarial perturbations</i>percentage of model inputs which were not preprocessed before reaching the production machine learning model. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the information system preprocesses all model inputs before they reach the production machine learning model to nullify or reverse potential adversarial perturbationsorganization checks user inputs (regardless of modality or source, including attachments) for anomalies and filters suspicious and/or unexpected values or patterns which could be adversarial or malicious in nature. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the identified anomalous entries are removedorganization checks user inputs (regardless of modality or source, including attachments) for anomalies and filters suspicious and/or unexpected values or patterns which could be adversarial or malicious in nature. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the identified anomalous entries are removed.
-------------------------------	--

Question Requirement Record: 07.10bAISecSystem.2 / 2872.0

Change Count: 4

Field	Content
BaselineUniqueld	07.10bA TL ASTLAS I SecISecSystem.2
RequirementStatement	<i>The organization, to detect and remove or remediate unsuitable and/or poisoned training data, inspects and sanitizes training data prior to model training and recurrently for an active learning model through statistical deviation or pattern recognition</i>The organization, to detect and remove or remediate unsuitable and/or poisoned training data, inspects and sanitizes training data prior to model training and recurrently for an active learning model through statistical deviation or pattern recognitionData for AI model training, AI model tuning, or prompt enhancement via RAG (if used) is checked prior to usage (e.g., using statistical methods, through manual inspection, or through automated means) for suspicious unexpected values or patterns which could be adversarial or malicious in nature (e.g., poisoned samples). Identified anomalous entries are removedData for AI model training, AI model tuning, or prompt enhancement via RAG (if used) is checked prior to usage (e.g., using statistical methods, through manual inspection, or through automated means) for suspicious unexpected values or patterns which could be adversarial or malicious in nature (e.g., poisoned samples). Identified anomalous entries are removed.

IllustrativeProcedureImplemented	For example, <i>select a sample of machine learning models and obtain and examine evidence to confirm machine learning models performed as intended prior to model training. Further select a sample of active learning models and obtain and examine evidence to confirm machine learning models were monitored recurrently. For any instances in which machine learning models were found to not perform as intended obtain and examine evidence to confirm removal or remediation of poisoned training data</i>select a sample of machine learning models and obtain and examine evidence to confirm machine learning models performed as intended prior to model training. Further select a sample of active learning models and obtain and examine evidence to confirm machine learning models were monitored recurrently. For any instances in which machine learning models were found to not perform as intended obtain and examine evidence to confirm removal or remediation of poisoned training datareview the AI system to ensure data for AI model training, AI model tuning, or prompt enhancement via RAG if used, is checked prior to usage for anomalies such as unexpected values or patterns (e.g., using statistical methods, through manual inspection). Further, confirm that the identified anomalous entries are removedreview the AI system to ensure data for AI model training, AI model tuning, or prompt enhancement via RAG if used, is checked prior to usage for anomalies such as unexpected values or patterns (e.g., using statistical methods, through manual inspection). Further, confirm that the identified anomalous entries are removed.
IllustrativeProcedureMeasured	For example, measures indicate if if the <i>number of instances where poisoned data was detected and removed or remediated. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization, to detect and remove or remediate unsuitable and/or poisoned training data, inspects and sanitizes training data prior to model training and recurrently for an active learning model</i>number of instances where poisoned data was detected and removed or remediated. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization, to detect and remove or remediate unsuitable and/or poisoned training data, inspects and sanitizes training data prior to model training and recurrently for an active learning modeldata for AI model training, AI model tuning, or prompt enhancement via RAG if used, is checked prior to usage for anomalies such as unexpected values or patterns (e.g., using statistical methods, through manual inspection). Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the identified anomalous entries are removeddata for AI model training, AI model tuning, or prompt enhancement via RAG if used, is checked prior to usage for anomalies such as unexpected values or patterns (e.g., using statistical methods, through manual inspection). Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the identified anomalous entries are removed.

Question Requirement Record: 07.10mATLASOrganizational.4 / 2871.0

Change Count: 3

Field	Content
RequirementStatement	<i>The information system uses multiple machine learning models to increase robustness to</i> The information system uses multiple machine learning models to increase robustness to Ensembling techniques are used to improve the robustness of the AI system against Ensembling techniques are used to improve the robustness of the AI system against attack.
IllustrativeProcedureImplemented	For example, <i>obtain and examine evidence to confirm the i</i> obtain and examine evidence to confirm the review the AI systems security configurations to coreview the AI systems security configurations to conf <i>o</i> irmation system uses multiple <i>machine learning models to increase robustness to</i> ation system uses multiple machine learning models to increase robustness to ensembling techniques are in place to improve the robustness of the AI system against ensembling techniques are in place to improve the robustness of the AI system against attack.
IllustrativeProcedureMeasured	For example, measures indicate if if the <i>use of multiple machine learning models for inference call</i> use of multiple machine learning models for inference call AI systems security configurations include ensembling technique AI systems security configurations include ensembling technique s. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and <i>to</i> to confirm the <i>organization uses multiple machine learning models to increase robustness to attack</i> e organization uses multiple machine learning models to increase robustness to attack at all AI systems utilize ensembling techniques at all AI systems utilize ensembling techniques.

Question Requirement Record: 07.10mAIISecOrganizational.6 / 2870.0

Change Count: 5

Field	Content
BaselineUniqueld	07.10mATLASISecOrganizational.3366

RequirementStatement	<i>The organization scans the machine learning artifacts (e.g., models and model architectures, the</i> organization scans the machine learning artifacts (e.g., models and model architectures, the o find potentially exploitable vulnerabilities, the organization inspects downloaded AI software assets before use—including models (e.g., such as those sourced from online model zoos); o find potentially exploitable vulnerabilities, the organization inspects downloaded AI software assets before use—including models (e.g., such as those sourced from online model zoos); software ~~st~~tpackagesages used to create, create, train,, and/or/or deploy models, <i>training and testing data, downloaded software,</i> training and testing data, downloaded software (e.g., python (e.g., python packages)); and <i>repositories) for vulnerabilities and signs of compromise before execution or use to find potentially exploitable software vulnerabilities in the AI system</i> repositories) for vulnerabilities and signs of compromise before execution or use to find potentially exploitable software vulnerabilities in the AI systemlanguage model tools such as agents and plugins (if used). The organization (4) acts upon the results, as necessarylanguage model tools such as agents and plugins (if used). The organization (4) acts upon the results, as necessary.
IllustrativeProcedureImplemented	For example, <i>obtain and examine evidence that machine learning artifacts (e.g., models and model architectures, the software stack used to train and deploy models, training and testing data, downloaded software packages and repositories) were scanned for vulnerabilities and signs of compromise before ex</i>obtain and examine evidence that machine learning artifacts (e.g., models and model architectures, the software stack used to train and deploy models, training and testing data, downloaded software packages and repositories) were scanned for vulnerabilities and signs of compromise before ex select a sample of downloaded AI software assets and confirm they were inspected before use. Further, confirm that the organization acts upon the inspselect a sample of downloaded AI software assets and confirm they were inspected before use. Further, confirm that the organization acts upon the inspecution or useor userresults, as necessary results, as necessary.

IllustrativeProcedureMeasured	For example, measures <i>could include the percentage of machine learning artifacts (e.g., models and model architectures, the software stack used to train and deploy models, training and testing data,</i> could include the percentage of machine learning artifacts (e.g., models and model architectures, the software stack used to train and deploy models, training and testing data, indicate percentage of the organization's indicate percentage of the organization's downloaded AI AI software <i>packages and repositories) which have not been scanned for vulnerabilities and signs of compromise as stipulated in the requirement statement. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization scans the machine learning artifacts (e.g., models and model architectures, the software stack used to train and deploy models, training and testing data, downloaded software packages and repositories) for vulnerabilities before execution or use to find potentially exploitable software vulnerabilities and signs of compromise in the AI system</i> packages and repositories) which have not been scanned for vulnerabilities and signs of compromise as stipulated in the requirement statement. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization scans the machine learning artifacts (e.g., models and model architectures, the software stack used to train and deploy models, training and testing data, downloaded software packages and repositories) for vulnerabilities before execution or use to find potentially exploitable software vulnerabilities and signs of compromise in the AI system assets that were not inspected before use. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that all AI software assets are inspected before use assets that were not inspected before use. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that all AI software assets are inspected before use.
DITA	Sampling Sampling

Question Requirement Record: 07.10mAIISecOrganizational.5 / 2867.0

Change Count: 4

Field	Content
BaselineUniqueld	07.10mATLASISecISecOrganizational.1155
RequirementStatement	To prevent against successful denial of AI service attacks and to hinder experimentation for AI attacks, to prevent against successful denial of AI service attacks and to hinder experimentation for AI attacks, the information system limits / throttles / throttles the total number and rate of API calls that a user can make to the AI <i>system</i>systemmodelmodel in a given time period.

IllustrativeProcedureImplemented	For example, <i>obtain and examine evidence to confirm that the organization limits the total number and rate of inference API calls possible</i> obtain and examine evidence to confirm that the organization limits the total number and rate of inference API calls possible review the AI model to ensure the system limits or throttles the total number and rate of API calls that a user can make to the AI model with review the AI model to ensure the system limits or throttles the total number and rate of API calls that a user can make to the AI model with in a given time time period.
IllustrativeProcedureMeasured	For example, measures indicate if if the <i>total number of API calls possible in a given period. Reviews, test</i> total number of API calls possible in a given period. Reviews, test system limits system limits,, or <i>audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization limits the total numbaudits are</i> completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization limits the total numb throttles the total number and rate of API calls that a u st throttles the total number and rate of API calls that a user ccand rate of inferenc d rate of inferenc make to th make to the APPI <i>calls</i> calls model with model within a given time time period <i>of time</i> of time.

Question Requirement Record: 19.09zAISecOrganizational.1 / 2866.0

Change Count: 4

Field	Content
BaselineUniqueld	19.09zA TLASTLASISecISecOrganizational.2211
RequirementStatement	The organization <i>restricrestriclimilimits the release of technical machine learning project details including data, algorithms,</i> machine learning project details including data, algorithms, AI project details, including specific information on the technical architecture of the overall AI system; datasets used for training, testing, validating, and tuning of confidential and/or closed-source AI models; datasets used for prompt augmentation via RAG (if performed); algorithm(s) used to create confidential and/or closed-source AIAI project details, including specific information on the technical architecture of the overall AI system; datasets used for training, testing, validating, and tuning of confidential and/or closed-source AI models; datasets used for prompt augmentation via RAG (if performed); algorithm(s) used to create confidential and/or closed-source AI models;s; architectures, model checkpoints,s, model checkpoints, of confidential and/or closed-source AI models; language model tools used such as agents and plugins (if used); safety and security checkpoints built into the AI system; of confidential and/or closed-source AI models; language model tools used such as agents and plugins (if used); safety and security checkpoints built into the AI system; and information on <i>the</i> the teams <i>supporting machine learning enabled products</i> supporting machine learning enabled products developing and supporting the AI system developing and supporting the AI system.

IllustrativeProcedureImplemented	For example, <i>obtain and examine process</i> obtain and examine process <i>examine released</i> examine released documentation <i>for</i> on the <i>public release of information and confirm the process includes a</i> public release of information and confirm the process includes a <i>AI system to ensure the organization</i> AI system to ensure the organization restriction <i>on</i> ion onss the release of <i>the</i> the technical <i>machine learning information as stipulat</i> machine learning information as stipulat <i>AI project details outlin</i> AI project details outlined in the requirement statement.
IllustrativeProcedureMeasured	For example, measures <i>could</i> could indicate the <i>existence of organizational machine learning information that has been publicly released. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization restricts the release of technical machine learning information as stipulated in</i> existence of organizational machine learning information that has been publicly released. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization restricts the release of technical machine learning information as stipulated in <i>amount of AI systems deployed by the company, of total, for which technical AI details have or have not been released in accordance with</i> amount of AI systems deployed by the company, of total, for which technical AI details have or have not been released in accordance with the <i>is</i> is requirement statement.

Question Requirement Record: 11.10hCISSystem.6 / 2856.0

Change Count: 1

Field	Content
BaselineUniqueld	11.01 <i>ICISOrganizational.1</i> 11ICISOrganizational.1 <i>10hCISSystem.6</i> 10hCISSystem.6

Question Requirement Record: 01.00aPCIOrganizational.3 / 2853.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate whether the PCI DSS scope was review <i>ed</i> by the organization within the last year and upon significant change to the in-scope environment. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization confirms PCI DSS scope annually and upon significant change to the in-scope environment.

Question Requirement Record: 19.13jPHIPAOrganizational.2 / 2735.0

Change Count: 1

Field	Content
BaselineUniqueld	19.13 <i>kkj</i> jPHIPAOrganizational. <i>33</i> 22

Question Requirement Record: 19.13kPHIPAOrganizational.1 / 2700.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of disclosures of relevant PHI to a person conducting an audit, reviewing an application for accreditation, or reviewing an accreditation and examine evidence to confirm the organization prevented the removal of the disclosed PHI from the organization's facility (unless the removal was authorized by law, or unless the person authorized the removal and provided that the records were held in a secure and confidential manner and were returned when the audit or review was completed).

Question Requirement Record: 19.13kPHIPAOrganizational.24 / 2751.0

Change Count: 1

Field	Content
BaselineUniqueld	19.13d ~~dk~~ kPHIPAOrganizational.332424

Question Requirement Record: 19.13aPHIPAOrganizational.3 / 2733.0

Change Count: 1

Field	Content
BaselineUniqueld	19.13b ~~ba~~ aPHIPAOrganizational.1133

Question Requirement Record: 15.13oPHIPAOrganizational.3 / 2692.0

Change Count: 1

Field	Content
BaselineUniqueld	15.11 ~~a~~ 1a3 ~~o~~ 3oPHIPAOrganizational.1133

Question Requirement Record: 08.09fTXRAMPSystem.2 / 2683.0

Change Count: 1

Field	Content
BaselineUniqueld	08.09m ~~mf~~ fTXRAMP ~~Organizational.1~~ Organizational.1System.2

Question Requirement Record: 01.04aNIST80053Organizational.3 / 2283.0

Change Count: 1

Field	Content
BaselineUniqueld	01310310.00044aNIST80053Organizational.5533

Question Requirement Record: 13.04aNIST80053Organizational.3 / 2577.0

Change Count: 1

Field	Content
BaselineUniqueld	13.02e2e4a4aNIST80053Organizational.1133

Question Requirement Record: 11.01qNIST80053System.3 / 2974.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the number of unmanaged elements specified in the requirement statement. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm the organization employs identity providers and authorization servers to manage user, device, and non-person entity identities, attributes, and access rights supporting authentication and authorization decisions in accordance with organization-defined identification and authentication policy using organization-defined mechanisms.

Question Requirement Record: 17.03dNIST80053Organizational.2 / 1984.0

Change Count: 1

Field	Content
BaselineUniqueld	17944944.03bbdNIST80053Organizational.1122

Question Requirement Record: 19.13iNIST80053Organizational.3 / 2288.0

Change Count: 1

Field	Content
BaselineUniqueld	19315.03a315.03a.13i.13iNIST80053Organizational.1133

Question Requirement Record: 19.13mNIST80053Organizational.3 / 2285.0

Change Count: 1

Field	Content
BaselineUniqueld	19312.03a312.03a.13m.13mNIST80053Organizational.2233

Question Requirement Record: 19.13hNIST80053Organizational.5 / 2315.0

Change Count: 1

Field	Content
BaselineUniqueld	19.10c0c3h3hNIST80053System.2System.2Organizational.5Organizational.5

Question Requirement Record: 15.11cNYDOHOrganizational.5 / 2214.0

Change Count: 1

Field	Content
BaselineUniqueld	15242242.11aaccNYDOHOrganizational.1155

Question Requirement Record: 06.09mNYDOHOrganizational.8 / 2201.0

Change Count: 1

Field	Content
BaselineUniqueld	06229.10hNYDOHSystem.4229.10hNYDOHSystem.4 .09mNYDOHOrganizational.8.09mNYDOHOrganizational.8

Question Requirement Record: 01.04aNYDOHOrganizational.2 / 2678.0

Change Count: 1

Field	Content
BaselineUniqueld	01.00044aNYDOHOrganizational.5522

Question Requirement Record: 17.03aNYDOHOrganizational.3 / 2082.0

Change Count: 1

Field	Content
BaselineUniqueld	17109109.03bbaNYDOHOrganizational.4433

Question Requirement Record: 13.13tNYDOHOrganizational.4 / 2075.0

Change Count: 1

Field	Content
BaselineUniqueld	13102.02e102.02e.13t.13tNYDOHOrganizational.6644

Question Requirement Record: 13.13tNYDOHOrganizational.3 / 2074.0

Change Count: 1

Field	Content
BaselineUniqueld	13101.02e101.02e.13t.13tNYDOHOrganizational.5533

Question Requirement Record: 191013.13bCCPAOrganizational.7 / 1937.0

Change Count: 1

Field	Content
RequirementStatement	Businesses which sell personal information to third-parties are required to provide a reasonably accessible notice to consumers that: provide a clear and conspicuous link on its website homepage, titled “ Do Not Sell My Limit the Use of My Sensitive Limit the Use of My Sensitive Personal Information,” which enables the consumer, or person authorized, to opt-out of the sale of personal information—the business may not require a consumer to open an account to exercise their opt-out right; include a description of the consumer’s rights and a separate link to the “ Do Not Sell My Limit the Use of My Sensitive Limit the Use of My Sensitive Personal Information” webpage in its online privacy notice or in any California-specific privacy notice; ensure that anyone who handles consumer inquiries knows the relevant requirements; refrain from selling information of a consumer who has opted-out; respect the consumer’s decision to opt-out for at least 12 months before seeking authorization to selling information again; and use personal information provided in an opt-out request only for complying with the request.

Question Requirement Record: 151207.11aSCIDSAOrganizational.2 / 1926.1

Change Count: 2

Field	Content
CrossVersionId	1926. 0011
RequirementStatement	The licensee provides, in electronic form, as much information as possible regarding the event, the date of the event, a description of what information was breached and how the information was breached, how the event was discovered, and and the number of total consumers in the state affected by the event, and a description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur , and a description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.

Question Requirement Record: 15.13oHIPAAOrganizational.2 / 2352.0

Change Count: 1

Field	Content
BaselineUniqueld	15.1 1a1a3o 3oHIPAAOrganizational. 7722

Question Requirement Record: 19.09abSRSystem.2 / 1952.0

Change Count: 1

Field	Content
BaselineUniqueld	19910.06cSROrganizational 910.06cSROrganizational .09abSRSystem .09abSRSystem.2

Question Requirement Record: 19.09dSRSystem.2 / 1951.0

Change Count: 1

Field	Content
BaselineUniqueld	19907.06cSROrganizational.5907.06cSROrganizational.5 .09dSRSystem.2.09dSRSystem.2

Question Requirement Record: 0963.10fCFRPart11Organizational.1 / 1291.0

Change Count: 1

Field	Content
RequirementStatement	The organization requires persons using electronic signatures to—prior to or at the time of such use—certify that the electronic signatures in their system—used on or after August 20, 1997—are intended to be the legally binding equivalent of traditional handwritten signatures. Such certification is required to be submitted in electronic or electronic or paper form and signed with a traditional handwritten signature, to the <i>Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857</i> Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857 FDA FDA. The organization also requires persons using electronic signatures to, upon request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signers hand-written signature.

Question Requirement Record: 19.13kHIPAAOrganizational.37 / 1609.0

Change Count: 1

Field	Content
BaselineUniqueld	19482482.13kTexasTexas HIPAA HIPAAOrganizational.252537 37

Question Requirement Record: 07.10mPCIOrganizational.4 / 2848.0

Change Count: 1

Field	Content
IllustrativeProcedureMeasured	For example, measures indicate the percentage of point of interaction devices which were not reviewed at the frequency or type as documented in the entity's targeted risk analy sis . Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization inspects point of interaction devices at a frequency and type as documented in the entity's targeted risk analysis.

Question Requirement Record: 19.09qPCIOrganizational.6 / 1033.0

Change Count: 1

Field	Content
BaselineUniqueld	030319.09qPCIOrganizational.6

Question Requirement Record: 19.09qPCIOrganizational.5 / 1032.0

Change Count: 1

Field	Content
BaselineUniqueld	031803181919.09qPCIOrganizational.34345

Question Requirement Record: 19.09qPCIOrganizational.4 / 1031.0

Change Count: 1

Field	Content
BaselineUniqueld	031703171919.09qPCIOrganizational.121244

Question Requirement Record: 15.08jFedRAMPOrganizational.3 / 1476.0

Change Count: 1

Field	Content
BaselineUniqueld	1585.11c85.11c.08j.08jFedRAMPOrganizational.4433

Question Requirement Record: 06.10kFedRAMPOrganizational.10 / 2454.0

Change Count: 3

Field	Content
RequirementStatement	The organization <i>audit</i> audit <i>monitor</i> monitors and reviews activities associated with configuration-controlled changes to the information system.
IllustrativeProcedureImplemented	For example, for a sample of activities associated with configuration-controlled changes to the information system obtain documentation that the changes were <i>audit</i> audit <i>monitor</i> monitored and reviewed.
IllustrativeProcedureMeasured	For example, measurements include the existence of documented <i>audits</i> audits <i>monitoring</i> monitoring and reviews of activities associated with configuration-controlled changes to the information system. Reviews, tests, or audits are completed by the organization to measure the effectiveness of the implemented controls and to confirm that the organization <i>audit</i> audit <i>monitor</i> monitors and reviews activities associated with configuration-controlled changes to the information system.

Question Requirement Record: 11.09mFedRAMPOrganizational.8 / 0158.0

Change Count: 1

Field	Content
BaselineUniqueld	11212.01/212.01l.09m.09mFedRAMPOrganizational.3388

Question Requirement Record: 11.10hFedRAMPSystem.2 / 0157.1

Change Count: 1

Field	Content
BaselineUniqueld	11205.01IFedRAMPOrganizational.4 205.01IFedRAMPOrganizational.4.10hFedRAMPSystem.2 .10hFedRAMPSystem.2

Question Requirement Record: 01.02fHIPAAOrganizational.3 / 0365.0

Change Count: 1

Field	Content
BaselineUniqueld	01108108.02fEHNAECEHNACHIPAAHIPAAOrganizational.113 3

Question Requirement Record: 13.02eCMSOrganizational.6 / 0352.0

Change Count: 1

Field	Content
BaselineUniqueld	133232.02eEHNAECEHNACMSCMSOrganizational.1166

Question Requirement Record: 03.09qCMSOrganizational.4 / 1006.0

Change Count: 1

Field	Content
BaselineUniqueld	031212.09ooqqCMSOrganizational.3344

Question Requirement Record: 03.09qCMSOrganizational.5 / 1079.0

Change Count: 1

Field	Content
BaselineUniqueld	032525.09uuqqCMSOrganizational.2255

Question Requirement Record: 19.13hCMSOrganizational.3 / 2514.0

Change Count: 1

Field	Content
BaselineUniqueld	19.13kkhhCMSOrganizational.1133

Question Requirement Record: 01.06dCMSOrganizational.2 / 2515.0

Change Count: 1

Field	Content
BaselineUniqueld	01.00a0a6d6dCMSOrganizational.2

Question Requirement Record: 01.04aCMSOrganizational.2 / 2513.0

Change Count: 1

Field	Content
BaselineUniqueld	01.00044aCMSOrganizational.1122

Question Requirement Record: 11.10hCMSSystem.3 / 1899.0

Change Count: 1

Field	Content
BaselineUniqueld	11..100.01ICMSOrganizational0.01ICMSOrganizational hCMSSystemhCMSSystem.344

Question Requirement Record: 19.13mCMSOrganizational.2 / 2535.0

Change Count: 1

Field	Content
BaselineUniqueld	19.03a03a13m13mCMSOrganizational.1122

Question Requirement Record: 17.09fCMSSystem.3 / 2668.0

Change Count: 1

Field	Content
BaselineUniqueld	17.03a3a9f9fCMSOrganizational.4Organizational.4System.3 System.3

Question Requirement Record: 1548.11c3Organizational.14 / 2020.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine evidence to determine if processes have been implemented for employing automated mechanisms to increase the availability of incident response-related information and support in accordance with the policy requirements and documented procedures (e.g., a website to query response-related information, or an automated mechanism that proactively sends incident response information to users) (e.g., a website to query response-related information, or an automated mechanism that proactively sends incident response information to users).

Question Requirement Record: 11.10h3System.2 / 0151.0

Change Count: 1

Field	Content
BaselineUniqueld	1196.01I3Organizational.10h3System.244

Question Requirement Record: 07.09m3Organizational.14 / 0635.0

Change Count: 1

Field	Content
BaselineUniqueld	0724.07a24.07a.09m.09m3Organizational.114

Question Requirement Record: 03.09o2Organizational.4 / 0999.0

Change Count: 1

Field	Content
BaselineUniqueld	030101.09o2Organizational.2244

Question Requirement Record: 08.09n2Organizational.8 / 0943.1

Change Count: 1

Field	Content
BaselineUniqueld	086565.09mmn2Organizational.141488

Question Requirement Record: 09.09o2Organizational.4 / 1058.0

Change Count: 1

Field	Content
BaselineUniqueld	091515.09sso2Organizational.2244

Question Requirement Record: 1520.11c2Organizational.4 / 1465.1

Change Count: 2

Field	Content
CrossVersionId	1465.0011
RequirementStatement	The organization disseminates incident response policy and procedures to appropriate elements within the organization. Responsible parties within the organization on a pre-defined frequency will review incident response policy and procedures. The organization communicates incident response policy and procedure changes to appropriate elements within the organization. The organization communicates incident response policy and procedure changes to appropriate elements within the organization.

Question Requirement Record: 1115.01h2Organizational.1 / 0115.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, tour the organization's facilities and observe the facilities' mail points to confirm that sensitive information is not visible through envelopes and marked according to classification level. Further, observe the incoming and outgoing mail points and facsimile machines to ensure that they are appropriately protected.

Question Requirement Record: 01.04a2Organizational.3 / 0298.0

Change Count: 1

Field	Content
BaselineUniqueld	013737.02244a2Organizational.3

Question Requirement Record: 11.02i2Organizational.5 / 0367.0

Change Count: 1

Field	Content
BaselineUniqueld	11144144.02ggi2Organizational.5

Question Requirement Record: 10902.01d1System.12 / 1945.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, select a sample of previously provided authentication credentials and determine if the credentials were provided securely (e.g., using an encrypted transmission) (e.g., using an encrypted transmission).

Question Requirement Record: 0613.06h1Organizational.12 / 0610.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine evidence to confirm that the organization performs annual technical compliance checks through manual or automated means (e.g., vulnerability scans, penetration testing, risk assessmentvulnerability scans, penetration testing, risk assessmenttechnical security configurations scantechnical security configurations scans). Select a sample of technical compliance checks and confirm that it is performed at least annually. Review the results of the annual technical compliance check and identify the areas of non-compliance. Select a sample of non-compliance and confirm that the organization performed the following: (i) performed root cause analysis to determine the causes of the non-compliance; (ii) evaluated the need for actions to ensure that non-compliance do not recur; (iii) implemented the appropriate corrective action; and, (iv) reviewed the corrective action taken.

Question Requirement Record: 19142.06c1Organizational.8 / 0558.0

Change Count: 1

Field	Content
IllustrativeProcedureImplemented	For example, examine the data retention and classification policies, procedures and processes to verify that guidelines are issued by the organization on the ownership, classification, retention, storage, handling, and disposal of ALL records and information. Further, select a sample of system components that store <i>organizational</i> organizational records and confirm that ownership, classification, retention, storage, handling and disposal requirements that have been appropriately assigned in accordance with the organization's policies.

Question Requirement Record: 06.09b1System.2 / 2368.0

Change Count: 2

Field	Content
RequirementStatement	Changes to information systems (including changes to applications, databases, configurations, <i>AI models</i> , AI models, network devices, and operating systems and with the potential exception of automated security patches) are consistently documented, tested, and approved.
IllustrativeProcedureImplemented	For example, select a sample of changes made to information systems (including changes to applications, databases, configurations, <i>AI models</i> , AI models, network devices, and operating systems and with the potential exception of automated security patches) and confirm that they were documented, tested, and approved.

Changes for Authoritative Source Document View D T O - v11.3.0 to v11.4.0

Authoritative Source Document View D T O: HITRUST Security for AI Systems

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	HITRUST Security for AI Systems

Authoritative Source Document View D T O: Federal Information Security Management Act (FISMA)

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	Federal Information Security Management Act (FISMA)

Authoritative Source Document View D T O: Cybersecurity Maturity Model Certification (CMMC) 2.0

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	Cybersecurity Maturity Model Certification (CMMC) 2.0

Authoritative Source Document View D T O: ISO/IEC 29151:2017 (Annex)

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	ISO/IEC 29151:2017 (Annex)

Authoritative Source Document View D T O: Digital Operational Resilience Act

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	Digital Operational Resilience Act

Authoritative Source Document View D T O: NAIC Insurance Data Security Model Law

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	NAIC Insurance Data Security Model Law

Authoritative Source Document View D T O: 21 CFR Part 11 (2024)

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	21 CFR Part 11 (2024)

Authoritative Source Document View D T O: California Consumer Privacy Act § 1798

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	California Consumer Privacy Act § 1798

Authoritative Source Document View D T O: State of Massachusetts Data Protection Act (201 CMR 17.00) 2024

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	State of Massachusetts Data Protection Act (201 CMR 17.00) 2024

Authoritative Source Document View D T O: CMS Acceptable Risk Safeguards (ARS) v5.1

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	CMS Acceptable Risk Safeguards (ARS) v5.1

Authoritative Source Document View D T O: NIST SP 800-171 r3

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	NIST SP 800-171 r3

Authoritative Source Document View D T O: 16 CFR 314: Standards for Safeguarding Customer Information

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	16 CFR 314: Standards for Safeguarding Customer Information

Authoritative Source Document View D T O: OWASP Machine Learning Security Top 10

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	OWASP Machine Learning Security Top 10

Authoritative Source Document View D T O: South Carolina Insurance Data Security Act (SCIDSA)

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	South Carolina Insurance Data Security Act (SCIDSA)

Authoritative Source Document View D T O: NIST Cybersecurity Framework 2.0

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	NIST Cybersecurity Framework 2.0

Authoritative Source Document View D T O: Texas Medical Records Privacy Act

Change Count: 0

Field	Content
New Authoritative Source Document View D T O	Texas Medical Records Privacy Act

Authoritative Source Document View D T O: NIST SP 800-172

Change Count: 2

Field	Content
Name	NIST SP SP 800-172
Description	NIST SP 800-17 1122 is a NIST Special Publication that provides enhanced security requirements for protecting the confidentiality of controlled unclassified information (CUI).

Authoritative Source Document View D T O: NY OHIP Moderate-Plus Security Baselines v5.0

Change Count: 2

Field	Content
Name	NY OHIP Moderate-Plus Security Baseline ss v5.0
ShortName	NY OHIP Moderate-Plus Security Baseline ss v5.0

Changes for Factor Type View D T O - v11.3.0 to v11.4.0

Factor Type View D T O: General - Organization Type

Change Count: 5

Field	Content
Name	Organization Type Organization Type
Description	Organization Type Organization Type
TypeOfInput	RR
Tooltip	Nature of the assessed entity's operations included in the scope of the assessment. Nature of the assessed entity's operations included in the scope of the assessment.
Order	0011

Factor Type View D T O: General - IaaS Provider

Change Count: 5

Field	Content
Name	IaaS Provider IaaS Provider
Description	Do you offer Infrastructure as a Service (IaaS)? Do you offer Infrastructure as a Service (IaaS)?
TypeOfInput	SS
Tooltip	Infrastructure as a service (IaaS) is a type of cloud computing service that offers essential compute, storage, and networking resources on demand, on a pay-as-you-go basis. Infrastructure as a service (IaaS) is a type of cloud computing service that offers essential compute, storage, and networking resources on demand, on a pay-as-you-go basis.
Order	0055

Factor Type View D T O: General - Group Health Plan

Change Count: 5

Field	Content
Name	Group Health Plan Group Health Plan
Description	Are you a Group Health Plan? Are you a Group Health Plan?
TypeOfInput	SS

Tooltip	An employee welfare benefit plan established or maintained by an employer or by an employee org., or both, that provides medical care for participants or their dependents directly or through insurance, reimbursement, or otherwise. An employee welfare benefit plan established or maintained by an employer or by an employee org., or both, that provides medical care for participants or their dependents directly or through insurance, reimbursement, or otherwise.
Order	0066

Factor Type View D T O: General - US Healthcare Entity Type

Change Count: 6

Field	Content
Name	US Healthcare Entity Type US Healthcare Entity Type
Description	Entity type designation in the US healthcare industry Entity type designation in the US healthcare industry
TypeOfInput	SS
Tooltip	The type of US healthcare organization as interpreted under HIPAA, specific to the assessed entity's operations included in the scope of the assessment. The type of US healthcare organization as interpreted under HIPAA, specific to the assessed entity's operations included in the scope of the assessment.
IsNonGraduated	Fals Fals Tru True
Order	110

Factor Type View D T O: Compliance - AI Risk Management

Change Count: 0

Field	Content
New Factor Type View D T O	Compliance - AI Risk Management

Factor Type View D T O: Compliance - AI Confidential parameters and technical architect

Change Count: 0

Field	Content
New Factor Type View D T O	Compliance - AI Confidential parameters and technical architect

Factor Type View D T O: Compliance - AI covered and/or confidential data

Change Count: 0

Field	Content
New Factor Type View D T O	Compliance - AI covered and/or confidential data

Factor Type View D T O: Compliance - What type of AI model(s) are used by in-scope IT platforms?
(select all that apply)

Change Count: 0

Field	Content
New Factor Type View D T O	Compliance - What type of AI model(s) are used by in-scope IT platforms? (select all that apply)

Factor Type View D T O: Compliance - Cybersecurity Maturity Model Certification (CMMC)

Change Count: 0

Field	Content
New Factor Type View D T O	Compliance - Cybersecurity Maturity Model Certification (CMMC)

Factor Type View D T O: Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1

Change Count: 0

Field	Content
New Factor Type View D T O	Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1

Factor Type View D T O: Compliance - StateRAMP r5

Change Count: 6

Field	Content
Name	StateRAMP r5 StateRAMP r5
Description	StateRAMP is built on the National Institute of Standards and Technology Special Publication 800-53 Rev. 5 framework, modeled in part after FedRAMP, and based on a “complete once, use many” concept that saves time and reduces costs for both service providers and governments. StateRAMP is built on the National Institute of Standards and Technology Special Publication 800-53 Rev. 5 framework, modeled in part after FedRAMP, and based on a “complete once, use many” concept that saves time and reduces costs for both service providers and governments.
TypeOfInput	NN
Tooltip	StateRAMP is built on the National Institute of Standards and Technology Special Publication 800-53 Rev. 5 framework, modeled in part after FedRAMP, and based on a “complete once, use many” concept that saves time and reduces costs for both service providers and governments. StateRAMP is built on the National Institute of Standards and Technology Special Publication 800-53 Rev. 5 framework, modeled in part after FedRAMP, and based on a “complete once, use many” concept that saves time and reduces costs for both service providers and governments.

IsNonGraduated	<i>Fals</i> Fals <i>Tru</i> True
Order	<i>0010</i> 15 1015

Factor Type View D T O: Compliance - HHS Cybersecurity Performance Goals

Change Count: 6

Field	Content
Name	HHS Cybersecurity Performance Goals HHS Cybersecurity Performance Goals
Description	HHS Cybersecurity Performance Goals HHS Cybersecurity Performance Goals
TypeOfInput	NN
Tooltip	The Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs) are designed to better protect the healthcare sector from cyberattacks, improve response when events occur, and minimize residual risk. HPH CPGs include both essential goals to outline minimum foundational practices for cybersecurity performance and enhanced goals to encourage adoption of more advanced practices. The Healthcare and Public Health (HPH) Cybersecurity Performance Goals (CPGs) are designed to better protect the healthcare sector from cyberattacks, improve response when events occur, and minimize residual risk. HPH CPGs include both essential goals to outline minimum foundational practices for cybersecurity performance and enhanced goals to encourage adoption of more advanced practices.
IsNonGraduated	<i>Fals</i> Fals <i>Tru</i> True
Order	<i>00100</i> 6 1006

Factor Type View D T O: Compliance - FFIEC CAT

Change Count: 6

Field	Content
Name	FFIEC CAT FFIEC CAT
Description	FFIEC Cybersecurity Assessment Tool FFIEC Cybersecurity Assessment Tool
TypeOfInput	NN
Tooltip	The FFIEC Cybersecurity Assessment Tool is based on the cybersecurity assessment that the FFIEC members piloted in 2014, which was designed to evaluate community institutions' preparedness to mitigate cyber risks. The FFIEC Cybersecurity Assessment Tool is based on the cybersecurity assessment that the FFIEC members piloted in 2014, which was designed to evaluate community institutions' preparedness to mitigate cyber risks.

IsNonGraduated	<i>Fals</i> Fals <i>Tru</i> True
Order	<i>001004</i> 1004

Factor Type View D T O: Compliance - CIS CSC v8.0

Change Count: 6

Field	Content
Name	CIS CSC v8.0 CIS CSC v8.0
Description	Center for Internet Security (CIS) Critical Security Controls (CSC) v8.0 Center for Internet Security (CIS) Critical Security Controls (CSC) v8.0
TypeOfInput	NN
Tooltip	Center for Internet Security (CIS) Critical Security Controls (CSC) v8.0 Center for Internet Security (CIS) Critical Security Controls (CSC) v8.0
IsNonGraduated	<i>Fals</i> Fals <i>Tru</i> True
Order	100 1000

Factor Type View D T O: Compliance - GDPR

Change Count: 6

Field	Content
Name	GDPR GDPR
Description	The General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR).
TypeOfInput	NN
Tooltip	The General Data Protection Regulation (GDPR) is a regulation on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals who are located in the EEA, and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of individuals inside the EEA. The General Data Protection Regulation (GDPR) is a regulation on data protection and privacy in the European Union (EU) and the European Economic Area (EEA). Superseding the Data Protection Directive 95/46/EC, the regulation contains provisions and requirements related to the processing of personal data of individuals who are located in the EEA, and applies to any enterprise—regardless of its location and the data subjects' citizenship or residence—that is processing the personal information of individuals inside the EEA.

IsNonGraduated	~~Fals~~ Fals Tru True
Order	~~001~~ 005 1005

Factor Type View D T O: Compliance - FedRAMP r5

Change Count: 6

Field	Content
Name	FedRAMP r5 FedRAMP r5
Description	The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security authorizations for cloud service offerings. FedRAMP is mandatory for all cloud services used by US Federal agencies. The Federal Risk and Authorization Management Program (FedRAMP) provides a standardized approach to security authorizations for cloud service offerings. FedRAMP is mandatory for all cloud services used by US Federal agencies.
TypeOfInput	NN
Tooltip	Federal Risk and Authorization Management Program (FedRAMP): Provides a standardized approach to security authorizations for cloud service offerings used by US Federal agencies. Federal Risk and Authorization Management Program (FedRAMP): Provides a standardized approach to security authorizations for cloud service offerings used by US Federal agencies.
IsNonGraduated	~~Fals~~ Fals Tru True
Order	~~001~~ 003 1003

Factor Type View D T O: Compliance - Ontario Personal Health Information Protection Act

Change Count: 6

Field	Content
Name	Ontario Personal Health Information Protection Act Ontario Personal Health Information Protection Act
Description	Ontario Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A; updated as of May 1, 2022 Ontario Personal Health Information Protection Act, 2004, S.O. 2004, c. 3, Sched. A; updated as of May 1, 2022
TypeOfInput	NN
Tooltip	The Personal Health Information Protection Act (PHIPA) is Ontario's health specific privacy legislation. PHIPA governs the manner in which personal health information may be collected, used and disclosed within the health sector. The Personal Health Information Protection Act (PHIPA) is Ontario's health specific privacy legislation. PHIPA governs the manner in which personal health information may be collected, used and disclosed within the health sector.

IsNonGraduated	<i>Fals</i> Fals <i>Tru</i> True
Order	<i>001014</i> 1014

Factor Type View D T O: Compliance - HICP 2023 Edition

Change Count: 6

Field	Content
Name	HICP 2023 Edition HICP 2023 Edition
Description	Health Industry Cybersecurity Practices 2023 Edition Health Industry Cybersecurity Practices 2023 Edition
TypeOfInput	NN
Tooltip	The HICP publication identifies five current cybersecurity threats and provides ten practices that can be used to mitigate them. It's comprised of a common set of cost-effective best practices based on widely accepted and used frameworks, standards, methodologies, processes, and procedures vetted by healthcare and security professionals. The HICP publication identifies five current cybersecurity threats and provides ten practices that can be used to mitigate them. It's comprised of a common set of cost-effective best practices based on widely accepted and used frameworks, standards, methodologies, processes, and procedures vetted by healthcare and security professionals.
IsNonGraduated	<i>Fals</i> Fals <i>Tru</i> True
Order	<i>001007</i> 1007

Factor Type View D T O: Compliance - NIST SP 800-53 R5

Change Count: 6

Field	Content
Name	NIST SP 800-53 R5 NIST SP 800-53 R5
Description	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5
TypeOfInput	NN

Tooltip	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations: Provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations: Provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
IsNonGraduated	~~Fals~~ Fals Tru True
Order	~~0010~~ 13 1013

Factor Type View D T O: Compliance - NIST SP 800-53 R4

Change Count: 6

Field	Content
Name	NIST SP 800-53 R4 NIST SP 800-53 R4
Description	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4
TypeOfInput	NN
Tooltip	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Information Systems and Organizations: Provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Security and Privacy Controls for Information Systems and Organizations: Provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS Publication 200, Minimum Security Requirements for Federal Information and Information Systems.
IsNonGraduated	~~Fals~~ Fals Tru True
Order	~~0010~~ 12 1012

Factor Type View D T O: Compliance - NIST SP 800-171 r2

Change Count: 6

Field	Content
Name	NIST SP 800-171 r2 NIST SP 800-171 r2
Description	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 2 National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 2
TypeOfInput	NN
Tooltip	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: NIST SP 800-171 is a NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI). National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: NIST SP 800-171 is a NIST Special Publication that provides recommended requirements for protecting the confidentiality of controlled unclassified information (CUI).
IsNonGraduated	Fals Fals Tru True
Order	001011 1011

Factor Type View D T O: Compliance - HIPAA

Change Count: 6

Field	Content
Name	HIPAA HIPAA
Description	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
TypeOfInput	NN
Tooltip	The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge.
IsNonGraduated	Fals Fals Tru True
Order	001008 1008

Factor Type View D T O: Compliance - HITRUST Reg: Compliance Factors

Change Count: 4

Field	Content
Name	HITRUST Reg: Compliance Factors HITRUST Reg: Compliance Factors
TypeOfInput	CC
IsNonGraduated	Fals Fals Tru True
Order	00274 274

Factor Type View D T O: Technical - HITRUST System: Wireless Access Points

Change Count: 5

Field	Content
Name	HITRUST System: Wireless Access Points HITRUST System: Wireless Access Points
Description	Are wireless access points in place at any of the organization's in-scope facilities? Are wireless access points in place at any of the organization's in-scope facilities?
TypeOfInput	SS
Tooltip	Are any wireless access points in place at any of the facilities included in the scope of the assessment? Wireless access points outside of the control of the organization, such as home and public wireless networks, should not be considered when answering this question. Wireless access points residing in in-scope, third-party-managed facilities (e.g., coworking facilities) which are controlled by a third-party (e.g., a coworking facility provider) should be considered when answering this question if they are known to be present.Are any wireless access points in place at any of the facilities included in the scope of the assessment? Wireless access points outside of the control of the organization, such as home and public wireless networks, should not be considered when answering this question. Wireless access points residing in in-scope, third-party-managed facilities (e.g., coworking facilities) which are controlled by a third-party (e.g., a coworking facility provider) should be considered when answering this question if they are known to be present.
Order	001007 1007

Factor Type View D T O: Technical - HITRUST System: Travel

Change Count: 5

Field	Content
Name	HITRUST System: Travel HITRUST System: Travel

Description	Do any of the organization's personnel travel to locations the organization deems to be of significant risk? Do any of the organization's personnel travel to locations the organization deems to be of significant risk?
TypeOfInput	SS
Tooltip	Do any of the organization's personnel travel to locations the organization deems to be of significant risk? Note that this is an entity-level consideration not specific to the facilities or platforms included in the scope of the assessment. Do any of the organization's personnel travel to locations the organization deems to be of significant risk? Note that this is an entity-level consideration not specific to the facilities or platforms included in the scope of the assessment.
Order	00 1004 1004

Factor Type View D T O: Technical - HITRUST System: Tokens

Change Count: 5

Field	Content
Name	HITRUST System: Tokens HITRUST System: Tokens
Description	Are hardware tokens used as an authentication method within the scoped environment? Are hardware tokens used as an authentication method within the scoped environment?
TypeOfInput	SS
Tooltip	Can hardware tokens be used to authenticate to any part of the scoped platforms? Hardware tokens are physical devices that provides a one-time key or nonce (e.g., PIV card, USB dongle, or fob). The use of mobile apps, email, and similar applications for two- or multi-factor authentication should be considered software tokens, not hardware tokens, when answering this question. Can hardware tokens be used to authenticate to any part of the scoped platforms? Hardware tokens are physical devices that provides a one-time key or nonce (e.g., PIV card, USB dongle, or fob). The use of mobile apps, email, and similar applications for two- or multi-factor authentication should be considered software tokens, not hardware tokens, when answering this question.
Order	00 1005 1005

Factor Type View D T O: Technical - HITRUST System: Third Party Exchange

Change Count: 5

Field	Content
Name	HITRUST System: Third Party Exchange HITRUST System: Third Party Exchange

Description	Does the system(s) transmit or receive data with a third-party? Does the system(s) transmit or receive data with a third-party?
TypeOfInput	SS
Tooltip	The in-scope information system(s) or application(s)exchanges information (interactively or through system-to-system connectivity) with a third-party (e.g., business partner, vendor, cloud service provider). Customers are considered "second parties", not "third parties" in this context and therefore should not be considered when answering this question. The in-scope information system(s) or application(s)exchanges information (interactively or through system-to-system connectivity) with a third-party (e.g., business partner, vendor, cloud service provider). Customers are considered "second parties", not "third parties" in this context and therefore should not be considered when answering this question.
Order	00258258

Factor Type View D T O: Technical - HITRUST System: Third Party Accessible

Change Count: 5

Field	Content
Name	HITRUST System: Third Party Accessible HITRUST System: Third Party Accessible
Description	Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)? Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?
TypeOfInput	SS

Tooltip	This parties are provided access into the in-scope information system(s) or application(s). A third-party is an entity that is separate from the assessed entity, that has been authorized for physical and/or logical access to the scoped system. This includes cloud service providers (as the provider would have relevant physical access). Furthermore, third-party accessibility does not depend on the means of access and occurs regardless of whether it is over a public network or whether the application is specifically hosted for customer use, for the purpose of operation, administration, or maintenance. Customers are considered "second parties", not "third parties" in this context and therefore should not be considered when answering this question. This parties are provided access into the in-scope information system(s) or application(s). A third-party is an entity that is separate from the assessed entity, that has been authorized for physical and/or logical access to the scoped system. This includes cloud service providers (as the provider would have relevant physical access). Furthermore, third-party accessibility does not depend on the means of access and occurs regardless of whether it is over a public network or whether the application is specifically hosted for customer use, for the purpose of operation, administration, or maintenance. Customers are considered "second parties", not "third parties" in this context and therefore should not be considered when answering this question.
Order	00257257

Factor Type View D T O: Technical - HITRUST System: Public Access

Change Count: 5

Field	Content
Name	HITRUST System: Public Access HITRUST System: Public Access
Description	Is the system(s) publicly positioned? Is the system(s) publicly positioned?
TypeOfInput	SS
Tooltip	The host organization has positioned the in-scope information system(s) or application(s) in a public location (e.g., as a kiosk in the welcome area of a hospital wing that lacks strict visitor control), which is distinct from a person using their own laptop to access their online bank account from a coffee shop. The host organization has positioned the in-scope information system(s) or application(s) in a public location (e.g., as a kiosk in the welcome area of a hospital wing that lacks strict visitor control), which is distinct from a person using their own laptop to access their online bank account from a coffee shop.
Order	00259259

Factor Type View D T O: Technical - HITRUST System: Number of users of the system

Change Count: 5

Field	Content
Name	HITRUST System: Number of users of the system HITRUST System: Number of users of the system
Description	Number of users of the system(s) Number of users of the system(s)
TypeOfInput	SS
Tooltip	The number of users that have access to the scoped information system(s), application(s), or service(s). The number of users that have access to the scoped information system(s), application(s), or service(s).
Order	00262 262

Factor Type View D T O: Technical - HITRUST System: Number of transactions per day

Change Count: 5

Field	Content
Name	HITRUST System: Number of transactions per day HITRUST System: Number of transactions per day
Description	Number of transactions per day Number of transactions per day
TypeOfInput	SS
Tooltip	The average number of transactions per day within the scoped information system(s), computed annually, where a transaction is defined as a discrete event between a user and a system that supports a business or programmatic purpose. The average number of transactions per day within the scoped information system(s), computed annually, where a transaction is defined as a discrete event between a user and a system that supports a business or programmatic purpose.
Order	00263 263

Factor Type View D T O: Technical - HITRUST System: Number of interfaces

Change Count: 5

Field	Content
Name	HITRUST System: Number of interfaces HITRUST System: Number of interfaces
Description	Number of interfaces to other systems Number of interfaces to other systems
TypeOfInput	SS

Tooltip	The number of interconnections (whether or not persistent) the scoped system(s) have with other systems, regardless of location, for the purpose of sharing data where the responsibility for security control lies outside the boundary of the existing system (whether with another part of the same organization or a third-party). The number of interconnections (whether or not persistent) the scoped system(s) have with other systems, regardless of location, for the purpose of sharing data where the responsibility for security control lies outside the boundary of the existing system (whether with another part of the same organization or a third-party).
Order	00261 261

Factor Type View D T O: Technical - HITRUST System: Internet

Change Count: 5

Field	Content
Name	HITRUST System: Internet HITRUST System: Internet
Description	Is the system(s) accessible from the Internet? Is the system(s) accessible from the Internet?
TypeOfInput	SS
Tooltip	Users are able to gain access to the in-scope information system(s) or application(s) from a public network (e.g., Internet). Applies whether the application is publicly exposed or is behind a firewall accessible only after first establishing access to an internal domain (e.g., VPN). Users are able to gain access to the in-scope information system(s) or application(s) from a public network (e.g., Internet). Applies whether the application is publicly exposed or is behind a firewall accessible only after first establishing access to an internal domain (e.g., VPN).
Order	00256 256

Factor Type View D T O: Technical - HITRUST System: Goods Services

Change Count: 5

Field	Content
Name	HITRUST System: Goods Services HITRUST System: Goods Services
Description	Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services? Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?
TypeOfInput	SS

Tooltip	Is any part of the scoped technology used by the organization to sell goods and/or services or to send or receive payment for goods and/or services? Is any part of the scoped technology used by the organization to sell goods and/or services or to send or receive payment for goods and/or services?
Order	001009 1009

Factor Type View D T O: Technical - HITRUST System: Fax

Change Count: 5

Field	Content
Name	HITRUST System: Fax HITRUST System: Fax
Description	Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)? Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?
TypeOfInput	SS
Tooltip	Does the scope of the assessment include any business processes which, in the normal course of business, feature the sending and/or receiving of confidential and/or covered information over fax machines (excludes efax and scan-to-email)? Does the scope of the assessment include any business processes which, in the normal course of business, feature the sending and/or receiving of confidential and/or covered information over fax machines (excludes efax and scan-to-email)?
Order	001003 1003

Factor Type View D T O: Technical - HITRUST System: External Access

Change Count: 5

Field	Content
Name	HITRUST System: External Access HITRUST System: External Access
Description	Does the system allow users to access the scoped environment from an external network that is not controlled by the organization? Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?
TypeOfInput	SS

Tooltip	Can any part of the scoped environment be accessed remotely from a network not controlled by the assessed entity? Examples include an employee connecting to an in-scope environment from a public wireless network or from their home and customers accessing an Internet-facing in-scope platform through a Web browser. The presence or absence of VPN or other secure tunneling technologies should not be considered when answering this question. Can any part of the scoped environment be accessed remotely from a network not controlled by the assessed entity? Examples include an employee connecting to an in-scope environment from a public wireless network or from their home and customers accessing an Internet-facing in-scope platform through a Web browser. The presence or absence of VPN or other secure tunneling technologies should not be considered when answering this question.
Order	001001 1001

Factor Type View D T O: Technical - HITRUST System: Electronic Signatures

Change Count: 5

Field	Content
Name	HITRUST System: Electronic Signatures HITRUST System: Electronic Signatures
Description	Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)? Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?
TypeOfInput	SS
Tooltip	Are electronic signatures used on or within any platforms, applications, or services included in the scope of the assessment? The use of electronic signatures includes, but is not limited to, e-prescription. Are electronic signatures used on or within any platforms, applications, or services included in the scope of the assessment? The use of electronic signatures includes, but is not limited to, e-prescription.
Order	101 1010

Factor Type View D T O: Technical - HITRUST System: Dial-Up

Change Count: 5

Field	Content
Name	HITRUST System: Dial-Up HITRUST System: Dial-Up

Description	Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)? Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?
TypeOfInput	SS
Tooltip	Are any analog modems functional within the scoped environment allowing dial-up/dial-in capabilities? Are any analog modems functional within the scoped environment allowing dial-up/dial-in capabilities?
Order	001002 1002

Factor Type View D T O: Technical - HITRUST System: Development

Change Count: 5

Field	Content
Name	HITRUST System: Development HITRUST System: Development
Description	Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component? Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?
TypeOfInput	SS
Tooltip	Information systems development refers to the practice of creating, testing, constructing, and/or introducing new computer systems, including, but not limited to, application, interface, database, and application programming interface (API) development. Information systems development refers to the practice of creating, testing, constructing, and/or introducing new computer systems, including, but not limited to, application, interface, database, and application programming interface (API) development.
Order	001008 1008

Factor Type View D T O: Technical - HITRUST System: Courier

Change Count: 5

Field	Content
Name	HITRUST System: Courier HITRUST System: Courier
Description	Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)? Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?
TypeOfInput	SS

Tooltip	Does the scope of the assessment include any business processes which, in the normal course of business, feature the sending and/or receiving of confidential and/or covered information over courier services, internal mail services, or external mail services (e.g., USPS)? Does the scope of the assessment include any business processes which, in the normal course of business, feature the sending and/or receiving of confidential and/or covered information over courier services, internal mail services, or external mail services (e.g., USPS)?
Order	00 1011 1011

Factor Type View D T O: Technical - HITRUST System: Cloud Hosted

Change Count: 5

Field	Content
Name	HITRUST System: Cloud Hosted HITRUST System: Cloud Hosted
Description	Is any aspect of the scoped environment hosted on the cloud? Is any aspect of the scoped environment hosted on the cloud?
TypeOfInput	SS
Tooltip	Is any aspect of the scoped environment hosted on a public, private, and/or hybrid cloud? Includes systems leveraging IaaS, PaaS, SaaS, and serverless technologies. Is any aspect of the scoped environment hosted on a public, private, and/or hybrid cloud? Includes systems leveraging IaaS, PaaS, SaaS, and serverless technologies.
Order	100 1000

Factor Type View D T O: Technical - HITRUST System: BYOD

Change Count: 5

Field	Content
Name	HITRUST System: BYOD HITRUST System: BYOD
Description	Does the organization allow personally-owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)? Does the organization allow personally-owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?
TypeOfInput	SS

Tooltip	Does the organization allow personally-owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)? Bring your own device (BYOD) include any devices outside of the organization's control that can be used to connect to organizational assets. Does the organization allow personally-owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)? Bring your own device (BYOD) include any devices outside of the organization's control that can be used to connect to organizational assets.
Order	00 1006 1006

Factor Type View D T O: Technical - AllSys

Change Count: 5

Field	Content
Name	AllSys AllSys
Description	Applicable to all systems Applicable to all systems
TypeOfInput	AA
Tooltip	Applicable to all systems / platforms included in the scope of the assessment. Applicable to all systems / platforms included in the scope of the assessment.
Order	00 999 999

Factor Type View D T O: Organizational - AllOrg

Change Count: 5

Field	Content
Name	AllOrg AllOrg
Description	Applicable to all Organizations Applicable to all Organizations
TypeOfInput	AA
Tooltip	Applicable to any organization undergoing a HITRUST assessment. Applicable to any organization undergoing a HITRUST assessment.
Order	00 999 999

Factor Type View D T O: Organizational - HITRUST Org New: Record Total

Change Count: 5

Field	Content
Name	HITRUST Org New: Record Total HITRUST Org New: Record Total

Description	Number of Records that are currently held: Number of Records that are currently held:
TypeOfInput	SS
Tooltip	Count of confidential and/or covered records stored on the platform(s) included in the scope of the assessment. Count of confidential and/or covered records stored on the platform(s) included in the scope of the assessment.
Order	00278 278

Factor Type View D T O: Organizational - HITRUST Org New: Record Count Annual

Change Count: 5

Field	Content
Name	HITRUST Org New: Record Count Annual HITRUST Org New: Record Count Annual
Description	Number of Individual Records that are processed annually: Number of Individual Records that are processed annually:
TypeOfInput	SS
Tooltip	Count of confidential and/or covered records received or transmitted yearly by the platform(s) included in the scope of the assessment. Count of confidential and/or covered records received or transmitted yearly by the platform(s) included in the scope of the assessment.
Order	00279 279

Factor Type View D T O: Organizational - HITRUST Org New: Physician Encounters

Change Count: 5

Field	Content
Name	HITRUST Org New: Physician Encounters HITRUST Org New: Physician Encounters
Description	Number of Patient Encounters Annually: Number of Patient Encounters Annually:
TypeOfInput	SS
Tooltip	Count of people that were provided care for in the year leading up to the assessment. Count of people that were provided care for in the year leading up to the assessment.
Order	00284 284

Factor Type View D T O: Organizational - HITRUST Org New: Physician Count

Change Count: 5

Field	Content
Name	HITRUST Org New: Physician Count HITRUST Org New: Physician Count
Description	Number of Physicians on staff: Number of Physicians on staff:
TypeOfInput	SS
Tooltip	Count of physicians employed. Count of physicians employed.
Order	00285 285

Factor Type View D T O: Organizational - HITRUST Org New: Pharmacy Companies

Change Count: 5

Field	Content
Name	HITRUST Org New: Pharmacy Companies HITRUST Org New: Pharmacy Companies
Description	Number of prescriptions filled annually: Number of prescriptions filled annually:
TypeOfInput	SS
Tooltip	Count of prescriptions directly or indirectly filled in the year leading up to the assessment. Count of prescriptions directly or indirectly filled in the year leading up to the assessment.
Order	00283 283

Factor Type View D T O: Organizational - HITRUST Org New: Non-IT Service Provider

Change Count: 5

Field	Content
Name	HITRUST Org New: Non-IT Service Provider HITRUST Org New: Non-IT Service Provider
Description	Volume of Data Exchanged Annually: Volume of Data Exchanged Annually:
TypeOfInput	SS
Tooltip	Megabytes of sensitive data exchanged in the year leading up to the assessment. Megabytes of sensitive data exchanged in the year leading up to the assessment.
Order	00288 288

Factor Type View D T O: Organizational - HITRUST Org New: IT Service Provider

Change Count: 5

Field	Content
Name	HITRUST Org New: IT Service Provider HITRUST Org New: IT Service Provider
Description	Total Terabytes of Data Held: Total Terabytes of Data Held:
TypeOfInput	SS
Tooltip	Total terabytes of data stored. Total terabytes of data stored.
Order	00287 287

Factor Type View D T O: Organizational - HITRUST Org New: Hospital Admissions

Change Count: 5

Field	Content
Name	HITRUST Org New: Hospital Admissions HITRUST Org New: Hospital Admissions
Description	Number of Admitted Patients annually: Number of Admitted Patients annually:
TypeOfInput	SS
Tooltip	Count of admitted patients in the year leading up to the assessment. Count of admitted patients in the year leading up to the assessment.
Order	00281 281

Factor Type View D T O: Organizational - HITRUST Org New: HIE Transactions

Change Count: 5

Field	Content
Name	HITRUST Org New: HIE Transactions HITRUST Org New: HIE Transactions
Description	Number of transactions received and sent annually: Number of transactions received and sent annually:
TypeOfInput	SS
Tooltip	Count of transactions received and sent in the year leading up to the assessment. Count of transactions received and sent in the year leading up to the assessment.
Order	00286 286

Factor Type View D T O: Organizational - HITRUST Org New: Health Plan/Insurance/PBM

Change Count: 5

Field	Content
Name	HITRUST Org New: Health Plan/Insurance/PBM HITRUST Org New: Health Plan/Insurance/PBM
Description	Number of Covered Lives: Number of Covered Lives:
TypeOfInput	SS
Tooltip	Count of lives covered by health insurance plans. “Covered life” means a subscriber, policyholder, certificate holder, spouse, dependent child or any other individual insured under an insurance policy or whose benefits are administered by a third party administrator. Count of lives covered by health insurance plans. “Covered life” means a subscriber, policyholder, certificate holder, spouse, dependent child or any other individual insured under an insurance policy or whose benefits are administered by a third party administrator.
Order	28 280

Factor Type View D T O: Organizational - HITRUST Org New: Bed

Change Count: 5

Field	Content
Name	HITRUST Org New: Bed HITRUST Org New: Bed
Description	Number of Licensed Beds: Number of Licensed Beds:
TypeOfInput	SS
Tooltip	Count of hospital beds available within the facilities included in the scope of the assessment. Count of hospital beds available within the facilities included in the scope of the assessment.
Order	00282 282

Changes for Factor View D T O - v11.3.0 to v11.4.0

Factor View D T O: General - Organization Type - Hospital / Inpatient Facility

Change Count: 4

Field	Content
Selection	Hospital / Inpatient Facility Hospital / Inpatient Facility
Order	0022
ToolTip	A facility for providing inpatient medical or surgical care. A facility for providing inpatient medical or surgical care.
SelectionLikelihood	0.04 .04

Factor View D T O: General - Organization Type - Federal Agency or Contractor

Change Count: 4

Field	Content
Selection	Federal Agency or Contractor Federal Agency or Contractor
Order	0088
ToolTip	Federal agency means any department, independent establishment, Government corporation, or other agency of the executive branch of the United States Federal Government, including the United States Postal Service. Federal contractors are entities that enter into a contractual agreement with any department or agency of the United States Government to perform a specific job, supply labor and/or materials, or for the sale of products and services. Federal agency means any department, independent establishment, Government corporation, or other agency of the executive branch of the United States Federal Government, including the United States Postal Service. Federal contractors are entities that enter into a contractual agreement with any department or agency of the United States Government to perform a specific job, supply labor and/or materials, or for the sale of products and services.
SelectionLikelihood	0.00 .00

Factor View D T O: General - Organization Type - Health Information Exchange (HIE)

Change Count: 4

Field	Content
Selection	Health Information Exchange (HIE) Health Information Exchange (HIE)
Order	0055

ToolTip	HIE is a term used to describe both the sharing of health information electronically among two or more entities and also a health information exchange organization that provides services that enable the sharing electronically of health information. HIE is a term used to describe both the sharing of health information electronically among two or more entities and also a health information exchange organization that provides services that enable the sharing electronically of health information.
SelectionLikelihood	0.03.03

Factor View D T O: General - Organization Type - Service Provider (Non-IT)

Change Count: 4

Field	Content
Selection	Service Provider (Non-IT) Service Provider (Non-IT)
Order	0077
ToolTip	Entities that provide non-IT services, such as transcription services and clearinghouses. Entities that provide non-IT services, such as transcription services and clearinghouses.
SelectionLikelihood	0.22.22

Factor View D T O: General - Organization Type - Service Provider (Information Technology, IT)

Change Count: 4

Field	Content
Selection	Service Provider (Information Technology, IT) Service Provider (Information Technology, IT)
Order	0066
ToolTip	Entities that provide IT services, such as Cloud services or hosted IT infrastructure. Entities that provide IT services, such as Cloud services or hosted IT infrastructure.
SelectionLikelihood	0.35.35

Factor View D T O: General - Organization Type - Physician Practice

Change Count: 4

Field	Content
Selection	Physician Practice Physician Practice
Order	0044
ToolTip	Medical practices comprised of one or more physicians organized to provide patient care services (regardless of its legal form or ownership). Medical practices comprised of one or more physicians organized to provide patient care services (regardless of its legal form or ownership).

SelectionLikelihood	0.02.02
---------------------	---------

Factor View D T O: General - Organization Type - Pharmacy / Pharmacy Benefit Management (PBM)

Change Count: 4

Field	Content
Selection	Pharmacy / Pharmacy Benefit Management (PBM) Pharmacy / Pharmacy Benefit Management (PBM)
Order	0033
ToolTip	Pharmacies are places where medicines are prepared, compounded, dispensed or sold. PBMs are companies that manage prescription drug benefits on behalf of health insurers, Medicare Part D drug plans, large employers, and other payers. Pharmacies are places where medicines are prepared, compounded, dispensed or sold. PBMs are companies that manage prescription drug benefits on behalf of health insurers, Medicare Part D drug plans, large employers, and other payers.
SelectionLikelihood	0.02.02

Factor View D T O: General - Organization Type - Payer

Change Count: 4

Field	Content
Selection	Payer Payer
Order	0011
ToolTip	Payers are covered entities identified as “Health Plans” under HIPAA, and are defined as an individual or group plan that provides, or pays the cost of, medical care. Health Insurance Exchanges (HIEs) are also considered payers for this purpose. (A health information exchange is an organization that provides services that enable the sharing electronically of health information.) Payers are covered entities identified as “Health Plans” under HIPAA, and are defined as an individual or group plan that provides, or pays the cost of, medical care. Health Insurance Exchanges (HIEs) are also considered payers for this purpose. (A health information exchange is an organization that provides services that enable the sharing electronically of health information.)
SelectionLikelihood	0.03.03

Factor View D T O: General - IaaS Provider - No

Change Count: 3

Field	Content
Selection	No No
Order	0022

SelectionLikelihood	0.29.29
---------------------	---------

Factor View D T O: General - IaaS Provider - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0011
SelectionLikelihood	0.06.06

Factor View D T O: General - Group Health Plan - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0011
SelectionLikelihood	0.03.03

Factor View D T O: General - Group Health Plan - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0022
SelectionLikelihood	0.01.01

Factor View D T O: General - US Healthcare Entity Type - Not a US healthcare entity

Change Count: 4

Field	Content
Selection	Not a US healthcare entityNot a US healthcare entity
Order	0044
ToolTip	Not a covered entity or business associate under HIPAA. Not a covered entity or business associate under HIPAA.
SelectionLikelihood	0.06.06

Factor View D T O: General - US Healthcare Entity Type - US Healthcare - Other

Change Count: 4

Field	Content
Selection	US Healthcare - Other US Healthcare - Other
Order	0033
ToolTip	Includes HIPAA hybrid entities (i.e. those that perform as both covered entities and business associates) as well as other healthcare entities whose operations are difficult to cleanly classify into either CE or BA. Includes HIPAA hybrid entities (i.e. those that perform as both covered entities and business associates) as well as other healthcare entities whose operations are difficult to cleanly classify into either CE or BA.
SelectionLikelihood	0.02 .02

Factor View D T O: General - US Healthcare Entity Type - US Healthcare - Covered Entity

Change Count: 4

Field	Content
Selection	US Healthcare - Covered Entity US Healthcare - Covered Entity
Order	0011
ToolTip	Health plans, health care clearinghouses, and health care providers in the US healthcare industry who electronically transmit any health information in connection with transactions for which HHS has adopted standards. Health plans, health care clearinghouses, and health care providers in the US healthcare industry who electronically transmit any health information in connection with transactions for which HHS has adopted standards.
SelectionLikelihood	0.15 .15

Factor View D T O: General - US Healthcare Entity Type - US Healthcare - Business Associate

Change Count: 4

Field	Content
Selection	US Healthcare - Business Associate US Healthcare - Business Associate
Order	0022
ToolTip	A US healthcare entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity. A US healthcare entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
SelectionLikelihood	0.49 .49

Factor View D T O: Compliance - AI Risk Management - NIST AI RMF & ISO/IEC 23894

Change Count: 5

Field	Content
Selection	NIST AI RMF & ISO/IEC 23894 NIST AI RMF & ISO/IEC 23894
Order	003333
ToolTip	Requirements focused on AI risk management, sourced from ISO/IEC 23894 and NIST AI Risk Management Framework Requirements focused on AI risk management, sourced from ISO/IEC 23894 and NIST AI Risk Management Framework
SelectionLikelihood	0.00.00
SupportsComplianceInsightsReporting	FalsFalsTruTrue

Factor View D T O: Compliance - AI Confidential parameters and technical architect - No

Change Count: 0

Field	Content
New Factor View D T O	Compliance - AI Confidential parameters and technical architect - No

Factor View D T O: Compliance - AI Confidential parameters and technical architect - Yes

Change Count: 0

Field	Content
New Factor View D T O	Compliance - AI Confidential parameters and technical architect - Yes

Factor View D T O: Compliance - AI covered and/or confidential data - No

Change Count: 0

Field	Content
New Factor View D T O	Compliance - AI covered and/or confidential data - No

Factor View D T O: Compliance - AI covered and/or confidential data - Yes

Change Count: 0

Field	Content
New Factor View D T O	Compliance - AI covered and/or confidential data - Yes

Factor View D T O: Compliance - What type of AI model(s) are used by in-scope IT platforms? (select all that apply) - Generative AI model

Change Count: 0

Field	Content
New Factor View D T O	Compliance - What type of AI model(s) are used by in-scope IT platforms? (select all that apply) - Generative AI model

Factor View D T O: Compliance - What type of AI model(s) are used by in-scope IT platforms? (select all that apply) - Predictive AI model

Change Count: 0

Field	Content
New Factor View D T O	Compliance - What type of AI model(s) are used by in-scope IT platforms? (select all that apply) - Predictive AI model

Factor View D T O: Compliance - What type of AI model(s) are used by in-scope IT platforms? (select all that apply) - Rule-based AI model

Change Count: 0

Field	Content
New Factor View D T O	Compliance - What type of AI model(s) are used by in-scope IT platforms? (select all that apply) - Rule-based AI model

Factor View D T O: Compliance - Cybersecurity Maturity Model Certification (CMMC) - Level 3

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Cybersecurity Maturity Model Certification (CMMC) - Level 3

Factor View D T O: Compliance - Cybersecurity Maturity Model Certification (CMMC) - Level 2

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Cybersecurity Maturity Model Certification (CMMC) - Level 2

Factor View D T O: Compliance - Cybersecurity Maturity Model Certification (CMMC) - Level 1

Change Count: 0

Field	Content
New Factor View D T O	Compliance - Cybersecurity Maturity Model Certification (CMMC) - Level 1

Factor View D T O: Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1 - HVA

Change Count: 0

Field	Content
New Factor View D T O	Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1 - HVA

Factor View D T O: Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1 - High

Change Count: 0

Field	Content
New Factor View D T O	Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1 - High

Factor View D T O: Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1 - Moderate

Change Count: 0

Field	Content
New Factor View D T O	Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1 - Moderate

Factor View D T O: Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1 - Low

Change Count: 0

Field	Content
New Factor View D T O	Compliance - CMS Acceptable Risk Safeguards (ARS) v5.1 - Low

Factor View D T O: Compliance - StateRAMP r5 - Impact level: Moderate

Change Count: 4

Field	Content
Selection	Impact level: Moderate Impact level: Moderate
Order	0022
ToolTip	A moderate-impact system is an information system in which at least one of the FIPS Publication 199 security objectives is moderate and no security objective is greater than moderate. A moderate-impact system is an information system in which at least one of the FIPS Publication 199 security objectives is moderate and no security objective is greater than moderate.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - StateRAMP r5 - Impact level: Low

Change Count: 4

Field	Content
Selection	Impact level: Low Impact level: Low

Order	0011
ToolTip	A low-impact system is defined as an information system in which all three of the FIPS Publication 199 security objectives are low. A low-impact system is defined as an information system in which all three of the FIPS Publication 199 security objectives are low.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HHS Cybersecurity Performance Goals - Enhanced Goals

Change Count: 4

Field	Content
Selection	Enhanced Goals Enhanced Goals
Order	0022
ToolTip	Enhanced Goals to help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors. Enhanced Goals to help healthcare organizations mature their cybersecurity capabilities and reach the next level of defense needed to protect against additional attack vectors.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HHS Cybersecurity Performance Goals - Essential Goals

Change Count: 4

Field	Content
Selection	Essential Goals Essential Goals
Order	0011
ToolTip	Essential Goals to help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyberattacks, improve response when events occur, and minimize residual risk. Essential Goals to help healthcare organizations address common vulnerabilities by setting a floor of safeguards that will better protect them from cyberattacks, improve response when events occur, and minimize residual risk.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - FFIEC CAT - Innovative

Change Count: 4

Field	Content
Selection	Innovative Innovative
Order	0055

ToolTip	Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses. Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyber risks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - FFIEC CAT - Advanced

Change Count: 4

Field	Content
Selection	Advanced Advanced
Order	0044
ToolTip	Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned. Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. Majority of risk-management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - FFIEC CAT - Intermediate

Change Count: 4

Field	Content
Selection	Intermediate Intermediate
Order	0033
ToolTip	Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies. Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk-management practices and analysis are integrated into business strategies.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - FFIEC CAT - Evolving

Change Count: 4

Field	Content
Selection	Evolving Evolving
Order	0022
ToolTip	Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems. Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - FFIEC CAT - Baseline

Change Count: 4

Field	Content
Selection	Baseline Baseline
Order	0011
ToolTip	Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance. Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - CIS CSC v8.0 - Implementation Group 3

Change Count: 4

Field	Content
Selection	Implementation Group 3 Implementation Group 3
Order	0033

ToolTip	An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - CIS CSC v8.0 - Implementation Group 2

Change Count: 4

Field	Content
Selection	Implementation Group 2 Implementation Group 2
Order	0022
ToolTip	An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - CIS CSC v8.0 - Implementation Group 1

Change Count: 4

Field	Content
Selection	Implementation Group 1 Implementation Group 1
Order	0011
ToolTip	An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - GDPR - Data Controller

Change Count: 4

Field	Content
Selection	Data Controller Data Controller

Order	0022
ToolTip	A data controller is a person or entity that determines how and why personal data is processed, including collecting, recording, disclosing, or deleting it. A data controller can be a legal person, such as a business, an SME, a public authority, or an agency. A data controller is a person or entity that determines how and why personal data is processed, including collecting, recording, disclosing, or deleting it. A data controller can be a legal person, such as a business, an SME, a public authority, or an agency.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - GDPR - Data Processor

Change Count: 4

Field	Content
Selection	Data Processor Data Processor
Order	0011
ToolTip	A data processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of a controller. A data processor acts under the controller's instructions and processes data, such as collection, storage, use, or disclosure. A data processor is a natural or legal person, public authority, agency, or other body that processes personal data on behalf of a controller. A data processor acts under the controller's instructions and processes data, such as collection, storage, use, or disclosure.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - FedRAMP r5 - High

Change Count: 4

Field	Content
Selection	High High
Order	0033
ToolTip	A high-impact system is an information system in which at least one FIPS Publication 199 security objective is high. A high-impact system is an information system in which at least one FIPS Publication 199 security objective is high.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - FedRAMP r5 - Moderate

Change Count: 4

Field	Content
Selection	Moderate Moderate

Order	0022
ToolTip	A moderate-impact system is an information system in which at least one of the FIPS Publication 199 security objectives is moderate and no security objective is greater than moderate. A moderate-impact system is an information system in which at least one of the FIPS Publication 199 security objectives is moderate and no security objective is greater than moderate.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - FedRAMP r5 - Low

Change Count: 4

Field	Content
Selection	LowLow
Order	0011
ToolTip	A low-impact system is defined as an information system in which all three of the FIPS Publication 199 security objectives are low. A low-impact system is defined as an information system in which all three of the FIPS Publication 199 security objectives are low.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - Ontario Personal Health Information Protection Act - Consumer Electronic Service Provider

Change Count: 5

Field	Content
Selection	Consumer Electronic Service Provider Consumer Electronic Service Provider
Order	0066
ToolTip	Consumer Electronic Service Provider Consumer Electronic Service Provider
SelectionLikelihood	0.00.00
SupportsComplianceInsightsReporting	FalsFals Tru True

Factor View D T O: Compliance - Ontario Personal Health Information Protection Act - Prescribed Organization

Change Count: 5

Field	Content
Selection	Prescribed Organization Prescribed Organization
Order	0055

ToolTip	Prescribed Organization Prescribed Organization
SelectionLikelihood	0.00.00
SupportsComplianceInsightsReporting	<i>Fals</i> Fals Tru True

Factor View D T O: Compliance - Ontario Personal Health Information Protection Act - Researcher

Change Count: 5

Field	Content
Selection	Researcher Researcher
Order	<i>00</i> 44
ToolTip	Researcher Researcher
SelectionLikelihood	0.00.00
SupportsComplianceInsightsReporting	<i>Fals</i> Fals Tru True

Factor View D T O: Compliance - Ontario Personal Health Information Protection Act - Agent

Change Count: 5

Field	Content
Selection	Agent Agent
Order	<i>00</i> 33
ToolTip	Agent Agent
SelectionLikelihood	0.00.00
SupportsComplianceInsightsReporting	<i>Fals</i> Fals Tru True

Factor View D T O: Compliance - Ontario Personal Health Information Protection Act - Health Data Institute

Change Count: 5

Field	Content
Selection	Health Data Institute Health Data Institute
Order	<i>00</i> 22
ToolTip	Health Data Institute Health Data Institute
SelectionLikelihood	0.00.00
SupportsComplianceInsightsReporting	<i>Fals</i> Fals Tru True

Factor View D T O: Compliance - Ontario Personal Health Information Protection Act - Health Information Custodian

Change Count: 5

Field	Content
Selection	Health Information Custodian Health Information Custodian
Order	0011
ToolTip	Health Information Custodian Health Information Custodian
SelectionLikelihood	0.00.00
SupportsComplianceInsightsReporting	Fals Fals Tru True

Factor View D T O: Compliance - HICP 2023 Edition - For Large Orgs.

Change Count: 4

Field	Content
Selection	For Large Orgs. For Large Orgs.
Order	0033
ToolTip	10 Cybersecurity Practices for large healthcare organizations 10 Cybersecurity Practices for large healthcare organizations
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HICP 2023 Edition - For Medium Orgs.

Change Count: 4

Field	Content
Selection	For Medium Orgs. For Medium Orgs.
Order	0022
ToolTip	10 Cybersecurity Practices for medium-sized healthcare organizations 10 Cybersecurity Practices for medium-sized healthcare organizations
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HICP 2023 Edition - For Small Orgs.

Change Count: 4

Field	Content
Selection	For Small Orgs. For Small Orgs.
Order	0011
ToolTip	10 Cybersecurity Practices for small healthcare organizations 10 Cybersecurity Practices for small healthcare organizations
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - NIST SP 800-53 R5 - Privacy

Change Count: 4

Field	Content
Selection	Privacy Privacy
Order	0055
ToolTip	A set of privacy controls based on international standards and best practices that help organizations enforce privacy requirements derived from federal legislation, directives, policies, regulations, and standards. A set of privacy controls based on international standards and best practices that help organizations enforce privacy requirements derived from federal legislation, directives, policies, regulations, and standards.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - NIST SP 800-53 R5 - Supplemental

Change Count: 4

Field	Content
Selection	Supplemental Supplemental
Order	0044
ToolTip	The supplemental guidance section provides non-prescriptive, additional information for a specific security control. Organizations can apply the supplemental guidance as appropriate, when defining, developing, and/or implementing security controls. The supplemental guidance can provide important considerations for implementing security controls in the context of operational environments, mission/business requirements, or assessments of risk and can also explain the purpose or meaning of particular controls. The supplemental guidance section provides non-prescriptive, additional information for a specific security control. Organizations can apply the supplemental guidance as appropriate, when defining, developing, and/or implementing security controls. The supplemental guidance can provide important considerations for implementing security controls in the context of operational environments, mission/business requirements, or assessments of risk and can also explain the purpose or meaning of particular controls.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - NIST SP 800-53 R5 - High

Change Count: 4

Field	Content
Selection	High High

Order	0033
ToolTip	A high-impact system is an information system in which at least one FIPS Publication 199 security objective is high. A high-impact system is an information system in which at least one FIPS Publication 199 security objective is high.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - NIST SP 800-53 R5 - Moderate

Change Count: 4

Field	Content
Selection	Moderate Moderate
Order	0022
ToolTip	A moderate-impact system is an information system in which at least one of the FIPS Publication 199 security objectives is moderate and no security objective is greater than moderate. A moderate-impact system is an information system in which at least one of the FIPS Publication 199 security objectives is moderate and no security objective is greater than moderate.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - NIST SP 800-53 R5 - Low

Change Count: 4

Field	Content
Selection	Low Low
Order	0011
ToolTip	A low-impact system is defined as an information system in which all three of the FIPS Publication 199 security objectives are low. A low-impact system is defined as an information system in which all three of the FIPS Publication 199 security objectives are low.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - NIST SP 800-53 R4 - Supplemental

Change Count: 4

Field	Content
Selection	Supplemental Supplemental
Order	0044

ToolTip	The supplemental guidance section provides non-prescriptive, additional information for a specific security control. Organizations can apply the supplemental guidance as appropriate, when defining, developing, and/or implementing security controls. The supplemental guidance can provide important considerations for implementing security controls in the context of operational environments, mission/business requirements, or assessments of risk and can also explain the purpose or meaning of particular controls. The supplemental guidance section provides non-prescriptive, additional information for a specific security control. Organizations can apply the supplemental guidance as appropriate, when defining, developing, and/or implementing security controls. The supplemental guidance can provide important considerations for implementing security controls in the context of operational environments, mission/business requirements, or assessments of risk and can also explain the purpose or meaning of particular controls.
SelectionLikelihood	0.01.01

Factor View D T O: Compliance - NIST SP 800-53 R4 - Privacy

Change Count: 4

Field	Content
Selection	Privacy Privacy
Order	0055
ToolTip	A set of privacy controls based on international standards and best practices that help organizations enforce privacy requirements derived from federal legislation, directives, policies, regulations, and standards. A set of privacy controls based on international standards and best practices that help organizations enforce privacy requirements derived from federal legislation, directives, policies, regulations, and standards.
SelectionLikelihood	0.01.01

Factor View D T O: Compliance - NIST SP 800-53 R4 - Moderate

Change Count: 4

Field	Content
Selection	Moderate Moderate
Order	0022
ToolTip	A moderate-impact system is an information system in which at least one of the FIPS Publication 199 security objectives is moderate and no security objective is greater than moderate. A moderate-impact system is an information system in which at least one of the FIPS Publication 199 security objectives is moderate and no security objective is greater than moderate.

SelectionLikelihood	0.02.02
---------------------	---------

Factor View D T O: Compliance - NIST SP 800-53 R4 - Low

Change Count: 4

Field	Content
Selection	LowLow
Order	0011
ToolTip	A low-impact system is defined as an information system in which all three of the FIPS Publication 199 security objectives are low. A low-impact system is defined as an information system in which all three of the FIPS Publication 199 security objectives are low.
SelectionLikelihood	0.02.02

Factor View D T O: Compliance - NIST SP 800-53 R4 - High

Change Count: 4

Field	Content
Selection	HighHigh
Order	0033
ToolTip	A high-impact system is an information system in which at least one FIPS Publication 199 security objective is high. A high-impact system is an information system in which at least one FIPS Publication 199 security objective is high.
SelectionLikelihood	0.01.01

Factor View D T O: Compliance - NIST SP 800-171 r2 - Derived Requirements

Change Count: 4

Field	Content
Selection	Derived RequirementsDerived Requirements
Order	0022

ToolTip	As explained in Section 2.2 of NIST SP 800-171, the derived requirements come from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. When the basic requirements do not fully meet the "Moderate" requirement, related controls from the "Moderate" baseline in NIST SP 800-53 are specified, and identified in NIST SP 800-171 as "derived requirements" (i.e., derived from NIST SP 800-53).As explained in Section 2.2 of NIST SP 800-171, the derived requirements come from NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations. When the basic requirements do not fully meet the "Moderate" requirement, related controls from the "Moderate" baseline in NIST SP 800-53 are specified, and identified in NIST SP 800-171 as "derived requirements" (i.e., derived from NIST SP 800-53).
SelectionLikelihood	0.02.02

Factor View D T O: Compliance - NIST SP 800-171 r2 - Basic Requirements

Change Count: 4

Field	Content
Selection	Basic Requirements Basic Requirements
Order	0011
ToolTip	As explained in Section 2.2 of NIST SP 800-171, the basic requirements come from FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. Since the FIPS 200 requirements are the most fundamental requirements, NIST 171 refers to them as "basic" requirements.As explained in Section 2.2 of NIST SP 800-171, the basic requirements come from FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. Since the FIPS 200 requirements are the most fundamental requirements, NIST 171 refers to them as "basic" requirements.
SelectionLikelihood	0.02.02

Factor View D T O: Compliance - HIPAA - HIPAA Security Rule

Change Count: 5

Field	Content
Selection	HIPAA Security Rule HIPAA Security Rule
Order	0022

ToolTip	The HIPAA Security Rule requires covered entities and business associates to protect patients' electronically stored, protected health information (known as "ePHI") by using appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of this information. The HIPAA Security Rule requires covered entities and business associates to protect patients' electronically stored, protected health information (known as "ePHI") by using appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of this information.
SelectionLikelihood	0. 48 .48
SupportsComplianceInsightsReporting	Fals Fals Tru True

Factor View D T O: Compliance - HIPAA - HIPAA Privacy Rule

Change Count: 5

Field	Content
Selection	HIPAA Privacy Rule HIPAA Privacy Rule
Order	00 11
ToolTip	The HIPAA Privacy Rule provides U.S. Federal standards to safeguard the privacy of personal health information and gives patients an array of rights with respect to that information, including rights to examine and obtain a copy of their health records and to request corrections. The HIPAA Privacy Rule provides U.S. Federal standards to safeguard the privacy of personal health information and gives patients an array of rights with respect to that information, including rights to examine and obtain a copy of their health records and to request corrections.
SelectionLikelihood	0. 19 .19
SupportsComplianceInsightsReporting	Fals Fals Tru True

Factor View D T O: Compliance - HIPAA - HIPAA Breach Notification

Change Count: 5

Field	Content
Selection	HIPAA Breach Notification HIPAA Breach Notification
Order	00 33

ToolTip	HIPAA's Breach Notification Rule requires covered entities and business associates to notify patients when their unsecured protected health information (PHI) is impermissibly used or disclosed—or “breached,”—in a way that compromises the privacy and security of the PHI. HIPAA's Breach Notification Rule requires covered entities and business associates to notify patients when their unsecured protected health information (PHI) is impermissibly used or disclosed—or “breached,”—in a way that compromises the privacy and security of the PHI.
SelectionLikelihood	0.29.29
SupportsComplianceInsightsReporting	~~Fals~~ Fals Tru True

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Security for AI Systems

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - Security for AI Systems

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NAIC Insurance Data Security Model Law

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - NAIC Insurance Data Security Model Law

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - ISO/IEC 29151:2017

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - ISO/IEC 29151:2017

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - DORA

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - DORA

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NIST SP 800-171 r3

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - NIST SP 800-171 r3

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - 16 CFR 314

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - 16 CFR 314

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - OWASP ML Top 10

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - OWASP ML Top 10

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NIST Cybersecurity Framework 2.0

Change Count: 0

Field	Content
New Factor View D T O	Compliance - HITRUST Reg: Compliance Factors - NIST Cybersecurity Framework 2.0

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NIST SP 800-172

Change Count: 4

Field	Content
Selection	NIST SP 800-172 NIST SP 800-172
Order	002727
ToolTip	National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172, which contains recommendations for enhanced security requirements to provide additional protection for Controlled Unclassified Information (CUI) in nonfederal systems and organizations when such information is associated with critical programs or high value assets. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-172, which contains recommendations for enhanced security requirements to provide additional protection for Controlled Unclassified Information (CUI) in nonfederal systems and organizations when such information is associated with critical programs or high value assets.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - MITRE ATLAS

Change Count: 4

Field	Content
Selection	MITRE ATLAS MITRE ATLAS
Order	0023 23
ToolTip	MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) is a globally accessible, living knowledge base of adversary tactics and techniques based on real-world attack observations and realistic demonstrations from AI red teams and security groups. MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) is a globally accessible, living knowledge base of adversary tactics and techniques based on real-world attack observations and realistic demonstrations from AI red teams and security groups.
SelectionLikelihood	0.00 .00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - OWASP AI Exchange

Change Count: 4

Field	Content
Selection	OWASP AI Exchange OWASP AI Exchange
Order	0029 29
ToolTip	The Open Worldwide Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. The OWASP AI Exchange was created to provide comprehensive guidance and alignment on how to protect AI against security threats--by professionals, for professionals. The Open Worldwide Application Security Project (OWASP) is a nonprofit foundation that works to improve the security of software. The OWASP AI Exchange was created to provide comprehensive guidance and alignment on how to protect AI against security threats--by professionals, for professionals.
SelectionLikelihood	0.00 .00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - PCI DSS v4.0

Change Count: 4

Field	Content
Selection	PCI DSS v4.0 PCI DSS v4.0
Order	0031 31

ToolTip	Payment Card Industry Data Security Standard (PCI DSS), Requirements and Security Assessment Procedures Version 4.0: The updated set of security standards originally formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express. Governed by the Payment Card Industry Security Standards Council (PCI SSC), the compliance scheme aims to secure credit and debit card transactions against data theft and fraud. Payment Card Industry Data Security Standard (PCI DSS), Requirements and Security Assessment Procedures Version 4.0: The updated set of security standards originally formed in 2004 by Visa, MasterCard, Discover Financial Services, JCB International and American Express. Governed by the Payment Card Industry Security Standards Council (PCI SSC), the compliance scheme aims to secure credit and debit card transactions against data theft and fraud.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - TX-RAMP 2.0

Change Count: 4

Field	Content
Selection	TX-RAMP 2.0 TX-RAMP 2.0
Order	440
ToolTip	In the 87th Legislative Session, the Texas Legislature passed Senate Bill 475, requiring the Texas Department of Information Resources (DIR) to establish a state risk and authorization management program that provides “a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency.” To comply, DIR established a framework for collecting information about cloud services security posture and assessing responses for compliance with required controls and documentation. In the 87th Legislative Session, the Texas Legislature passed Senate Bill 475, requiring the Texas Department of Information Resources (DIR) to establish a state risk and authorization management program that provides “a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency.” To comply, DIR established a framework for collecting information about cloud services security posture and assessing responses for compliance with required controls and documentation.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - ISO 31000:2018

Change Count: 4

Field	Content
Selection	ISO 31000:2018 ISO 31000:2018

Order	002121
ToolTip	Risk Management: Provides guidelines on managing risk faced by organizations, a common approach to managing any type of risk and is not industry or sector specific, and can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels. Risk Management: Provides guidelines on managing risk faced by organizations, a common approach to managing any type of risk and is not industry or sector specific, and can be used throughout the life of the organization and can be applied to any activity, including decision-making at all levels.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - NY OHIP Moderate-plus Security Baselines v5.0

Change Count: 4

Field	Content
Selection	NY OHIP Moderate-plus Security Baselines v5.0 NY OHIP Moderate-plus Security Baselines v5.0
Order	002828

ToolTip	NYS Department of Health (NY DOH) Office of Health Insurance Programs (OHIP) Division of Operations and Systems (DOS) System Security Plan (SSP) Overview Document V5.0: New York State Office of Health Insurance Programs (OHIP) is responsible for providing guidance and oversight for Medicaid related information systems, programs, and business processes at the Department of Health (DOH). This responsibility includes defining business, information, and technical guidance that will create a common security framework for IT system implementations responsible for protecting DOH Medicaid data. OHIP extends this guidance to entities with whom DOH provided Medicaid data is shared. The guidance and security framework is based on the set of NIST 800-53 recommended security controls for government information systems at the moderate level with enhancements that are necessary to comply with NYS Policies and Standards (aka Moderate Plus). NYS Department of Health (NY DOH) Office of Health Insurance Programs (OHIP) Division of Operations and Systems (DOS) System Security Plan (SSP) Overview Document V5.0: New York State Office of Health Insurance Programs (OHIP) is responsible for providing guidance and oversight for Medicaid related information systems, programs, and business processes at the Department of Health (DOH). This responsibility includes defining business, information, and technical guidance that will create a common security framework for IT system implementations responsible for protecting DOH Medicaid data. OHIP extends this guidance to entities with whom DOH provided Medicaid data is shared. The guidance and security framework is based on the set of NIST 800-53 recommended security controls for government information systems at the moderate level with enhancements that are necessary to comply with NYS Policies and Standards (aka Moderate Plus).
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - ISO/IEC 27002:2022

Change Count: 4

Field	Content
Selection	ISO/IEC 27002:2022 ISO/IEC 27002:2022
Order	001919
ToolTip	Information Security, Cybersecurity And Privacy Protection — Information Security Controls: Provides a reference set of generic information security controls including implementation guidance. Information Security, Cybersecurity And Privacy Protection — Information Security Controls: Provides a reference set of generic information security controls including implementation guidance.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - VA Directive 6500

Change Count: 4

Field	Content
Selection	VA Directive 6500 VA Directive 6500
Order	0041 41
ToolTip	The purpose of the VA cybersecurity and privacy program is to set the direction for the protection and informed risk management of VA information and VA Information System (IS). The purpose of the VA cybersecurity and privacy program is to set the direction for the protection and informed risk management of VA information and VA Information System (IS).
SelectionLikelihood	0.00 .00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - ISO/IEC 27001:2022

Change Count: 4

Field	Content
Selection	ISO/IEC 27001:2022 ISO/IEC 27001:2022
Order	0018 18
ToolTip	Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements: Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements: Specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization.
SelectionLikelihood	0.00 .00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - MARS-E v2.2

Change Count: 4

Field	Content
Selection	MARS-E v2.2 MARS-E v2.2
Order	0022 22

ToolTip	For the protection of the security and privacy of information systems in the Affordable Care Act (ACA) program environment, the Centers for Medicare & Medicaid Services (CMS) has assembled a document suite of guidance, requirements, and templates known as the Minimum Acceptable Risk Standards for Exchanges (MARS-E), v. 2.2. For the protection of the security and privacy of information systems in the Affordable Care Act (ACA) program environment, the Centers for Medicare & Medicaid Services (CMS) has assembled a document suite of guidance, requirements, and templates known as the Minimum Acceptable Risk Standards for Exchanges (MARS-E), v. 2.2.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Legacy Inheritance Support

Change Count: 4

Field	Content
Selection	Legacy Inheritance Support Legacy Inheritance Support
Order	00999999
ToolTip	Includes fully and partially inheritable HITRUST CSF requirements found in the baseline of r2 assessments using any 9.x version of the HITRUST CSF but not found in the v11 r2 assessment baseline. Includes fully and partially inheritable HITRUST CSF requirements found in the baseline of r2 assessments using any 9.x version of the HITRUST CSF but not found in the v11 r2 assessment baseline.
SelectionLikelihood	0.00.00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - State of Nevada Security and Privacy of Personal Information

Change Count: 4

Field	Content
Selection	State of Nevada Security and Privacy of Personal Information State of Nevada Security and Privacy of Personal Information
Order	003535
ToolTip	Nevada Revised Statutes (NRS) Chapter 603A, Security and Privacy of Personal Information, Security of Information Maintained by Data Collectors and Other Businesses: Set of security and privacy requirements for receiving, storing, or processing personal information for the residents of the state of Nevada. Nevada Revised Statutes (NRS) Chapter 603A, Security and Privacy of Personal Information, Security of Information Maintained by Data Collectors and Other Businesses: Set of security and privacy requirements for receiving, storing, or processing personal information for the residents of the state of Nevada.

SelectionLikelihood	0.03.03
---------------------	---------

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - PDPA (Singapore)

Change Count: 4

Field	Content
Selection	PDPA (Singapore) PDPA (Singapore)
Order	003232
ToolTip	Republic of Singapore, Personal Data Protection Act of 2012 (PDPA): Provides a baseline standard of protection for personal data in Singapore. Republic of Singapore, Personal Data Protection Act of 2012 (PDPA): Provides a baseline standard of protection for personal data in Singapore.
SelectionLikelihood	0.03.03

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Texas Medical Records Privacy Act

Change Count: 4

Field	Content
Selection	Texas Medical Records Privacy Act Texas Medical Records Privacy Act
Order	003737
ToolTip	Texas Health and Safety Code, Title 2: Health, Subtitle I: Medical Records, Chapter 181: Medical Records Privacy: The Texas Medical Records Privacy Act (TMRPA), or the "Texas privacy act" was introduced to safeguard Protected Health Information (PHI), which relates to the past, present, or future health of an individual; the provision of healthcare to an individual; or the payment for the provision of healthcare to an individual. The Texas privacy act has also adopted the term "covered entity", which includes hospitals, insurance providers, health maintenance organizations, clearing-houses, and other service providers that handle PHI. Texas Health and Safety Code, Title 2: Health, Subtitle I: Medical Records, Chapter 181: Medical Records Privacy: The Texas Medical Records Privacy Act (TMRPA), or the "Texas privacy act" was introduced to safeguard Protected Health Information (PHI), which relates to the past, present, or future health of an individual; the provision of healthcare to an individual; or the payment for the provision of healthcare to an individual. The Texas privacy act has also adopted the term "covered entity", which includes hospitals, insurance providers, health maintenance organizations, clearing-houses, and other service providers that handle PHI.
SelectionLikelihood	0.02.02

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Supplemental Requirements

Change Count: 4

Field	Content
Selection	Supplemental Requirements Supplemental Requirements
Order	003636
ToolTip	Community Supplemental Requirements #1: Contact Support@hitrustalliance.net to request more information about this source. Community Supplemental Requirements #1: Contact Support@hitrustalliance.net to request more information about this source.
SelectionLikelihood	0.01.01

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - State of Massachusetts Data Protection Act (201 CMR 17.00)

Change Count: 4

Field	Content
Selection	State of Massachusetts Data Protection Act (201 CMR 17.00) State of Massachusetts Data Protection Act (201 CMR 17.00)
Order	003434
ToolTip	Office for Consumer Affairs and Business Regulations, Standards for the Protection of Personal Information of Residents of the Commonwealth: The Massachusetts Data Protection Act is legislation that stipulates security requirements for organizations that handle the private data of residents. The law is more formally known as "Standards for The Protection of Personal Information of Residents of the Commonwealth" (or 201 CMR 17.00). Office for Consumer Affairs and Business Regulations, Standards for the Protection of Personal Information of Residents of the Commonwealth: The Massachusetts Data Protection Act is legislation that stipulates security requirements for organizations that handle the private data of residents. The law is more formally known as "Standards for The Protection of Personal Information of Residents of the Commonwealth" (or 201 CMR 17.00).
SelectionLikelihood	0.05.05

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - SCIDSA

Change Count: 4

Field	Content
Selection	SCIDSA SCIDSA
Order	003333

ToolTip	South Carolina Insurance Data Security Act (SCIDSA): A data security/compliance law targeting insurance industry-related businesses operating in South Carolina and those persons licensed to operate by the South Carolina Department of Insurance (DOI). South Carolina Insurance Data Security Act (SCIDSA): A data security/compliance law targeting insurance industry-related businesses operating in South Carolina and those persons licensed to operate by the South Carolina Department of Insurance (DOI).
SelectionLikelihood	0.02.02

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - California Consumer Privacy Act § 1798

Change Count: 4

Field	Content
Selection	California Consumer Privacy Act § 1798 California Consumer Privacy Act § 1798
Order	0055
ToolTip	California Consumer Privacy Act of 2018 (CCPA): Intended to apply to any profit or non-profit organization located anywhere in the world that collects personal information about a California resident; supports the CA Attorney General's interpretation of "reasonable security". California Consumer Privacy Act of 2018 (CCPA): Intended to apply to any profit or non-profit organization located anywhere in the world that collects personal information about a California resident; supports the CA Attorney General's interpretation of "reasonable security".
SelectionLikelihood	0.03.03

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - 23 NYCRR 500 Second Amendment

Change Count: 4

Field	Content
Selection	23 NYCRR 500 Second Amendment 23 NYCRR 500 Second Amendment
Order	0033
ToolTip	New York Codes, Rules and Regulations (NYCRR) Title 23 Part 500, "Cybersecurity Requirements for Financial Services Companies": Aims to protect consumers and to "ensure the safety and soundness of the institution on behalf of their clients," through regulations around cybersecurity. New York Codes, Rules and Regulations (NYCRR) Title 23 Part 500, "Cybersecurity Requirements for Financial Services Companies": Aims to protect consumers and to "ensure the safety and soundness of the institution on behalf of their clients," through regulations around cybersecurity.

SelectionLikelihood	0.03.03
---------------------	---------

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - 21 CFR Part 11

Change Count: 4

Field	Content
Selection	21 CFR Part 11 21 CFR Part 11
Order	0022
ToolTip	U.S. Food and Drug Administration (FDA) Part 11, Electronic Records; Electronic Signatures - Scope and Application: Provides guidance to persons who, in fulfillment of a requirement in a statute or another part of FDA's regulations to maintain records or submit information to FDA, have chosen to maintain the records or submit designated information electronically and, as a result, have become subject to part 11. Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations. Part 11 also applies to electronic records submitted to the Agency under the Federal Food, Drug, and Cosmetic Act (the Act) and the Public Health Service Act (the PHS Act), even if such records are not specifically identified in Agency regulations (§ 11.1).U.S. Food and Drug Administration (FDA) Part 11, Electronic Records; Electronic Signatures - Scope and Application: Provides guidance to persons who, in fulfillment of a requirement in a statute or another part of FDA's regulations to maintain records or submit information to FDA, have chosen to maintain the records or submit designated information electronically and, as a result, have become subject to part 11. Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations. Part 11 also applies to electronic records submitted to the Agency under the Federal Food, Drug, and Cosmetic Act (the Act) and the Public Health Service Act (the PHS Act), even if such records are not specifically identified in Agency regulations (§ 11.1).
SelectionLikelihood	0.04.04

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - The Joint Commission v2016

Change Count: 4

Field	Content
Selection	The Joint Commission v2016 The Joint Commission v2016
Order	003838

ToolTip	The Joint Commission (TJC), Program: Hospital, Chapter: Information Management (IM), January 1, 2016: A set of security and privacy standards published by The Joint Commission on Accreditation of Healthcare Organizations. The Joint Commission (TJC), Program: Hospital, Chapter: Information Management (IM), January 1, 2016: A set of security and privacy standards published by The Joint Commission on Accreditation of Healthcare Organizations.
SelectionLikelihood	0.02.02

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - IRS Pub. 1075

Change Count: 4

Field	Content
Selection	IRS Pub. 1075 IRS Pub. 1075
Order	001717
ToolTip	Tax Information Security Guidelines For Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information: Controls required for protection of Federal Tax Information (FTI). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS) or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC § 6103(p)(2)(B) Agreement. FTI is categorized as Sensitive But Unclassified (SBU) information and may contain personally identifiable information (PII). Tax Information Security Guidelines For Federal, State, and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information: Controls required for protection of Federal Tax Information (FTI). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS) or Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to an IRC § 6103(p)(2)(B) Agreement. FTI is categorized as Sensitive But Unclassified (SBU) information and may contain personally identifiable information (PII).
SelectionLikelihood	0.01.01

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - HITRUST De-ID Framework

Change Count: 4

Field	Content
Selection	HITRUST De-ID Framework HITRUST De-ID Framework
Order	001616

ToolTip	HITRUST De-Identification (De-ID) Framework: Generally used to assess the protections afforded through a de-identified data set in its intended use environment (e.g., processed, stored, transmitted). HITRUST De-Identification (De-ID) Framework: Generally used to assess the protections afforded through a de-identified data set in its intended use environment (e.g., processed, stored, transmitted).
SelectionLikelihood	0.03.03

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - FTC Red Flags Rule (16 CFR 681)

Change Count: 4

Field	Content
Selection	FTC Red Flags Rule (16 CFR 681) FTC Red Flags Rule (16 CFR 681)
Order	001515
ToolTip	Federal Trade Commission (FTC) Red Flags Rule: Requires SEC-regulated entities that qualify as financial institutions or creditors under FCRA to implement a written Identity Theft Prevention Program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations. Federal Trade Commission (FTC) Red Flags Rule: Requires SEC-regulated entities that qualify as financial institutions or creditors under FCRA to implement a written Identity Theft Prevention Program designed to detect the warning signs – or red flags – of identity theft in their day-to-day operations.
SelectionLikelihood	00-1.99-1.99

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - FISMA

Change Count: 4

Field	Content
Selection	FISMA FISMA
Order	001414
ToolTip	Federal Information Security Management Act (FISMA): United States legislation that defines a framework of guidelines and security standards to protect U.S. government information and operations. It contains compulsory requirements for the security of government information systems, that also apply to third-party service providers. Federal Information Security Management Act (FISMA): United States legislation that defines a framework of guidelines and security standards to protect U.S. government information and operations. It contains compulsory requirements for the security of government information systems, that also apply to third-party service providers.
SelectionLikelihood	0.02.02

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Data Governance Framework

Change Count: 4

Field	Content
Selection	Data Governance Framework Data Governance Framework
Order	1 10
ToolTip	Contact Support@hitrustalliance.net to request more information about this source. Contact Support@hitrustalliance.net to request more information about this source.
SelectionLikelihood	0.00 .00

Factor View D T O: Compliance - HITRUST Reg: Compliance Factors - Community Supplemental Requirements 002

Change Count: 4

Field	Content
Selection	Community Supplemental Requirements 002 Community Supplemental Requirements 002
Order	00 88
ToolTip	Community Supplemental Requirements #2 (v2018): Contact Support@hitrustalliance.net to request more information about this source. Community Supplemental Requirements #2 (v2018): Contact Support@hitrustalliance.net to request more information about this source.
SelectionLikelihood	0.01 .01

Factor View D T O: Technical - HITRUST System: Wireless Access Points - Yes

Change Count: 3

Field	Content
Selection	Yes Yes
Order	00 22
SelectionLikelihood	0.47 .47

Factor View D T O: Technical - HITRUST System: Wireless Access Points - No

Change Count: 3

Field	Content
Selection	No No
Order	00 11

SelectionLikelihood	0.24.24
---------------------	---------

Factor View D T O: Technical - HITRUST System: Travel - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.63.63

Factor View D T O: Technical - HITRUST System: Travel - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.08.08

Factor View D T O: Technical - HITRUST System: Tokens - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.54.54

Factor View D T O: Technical - HITRUST System: Tokens - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.17.17

Factor View D T O: Technical - HITRUST System: Third Party Exchange - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022

SelectionLikelihood	0.60.60
---------------------	---------

Factor View D T O: Technical - HITRUST System: Third Party Exchange - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.11.11

Factor View D T O: Technical - HITRUST System: Third Party Accessible - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.10.10

Factor View D T O: Technical - HITRUST System: Third Party Accessible - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.61.61

Factor View D T O: Technical - HITRUST System: Public Access - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.25.25

Factor View D T O: Technical - HITRUST System: Public Access - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011

SelectionLikelihood	0.46.46
---------------------	---------

Factor View D T O: Technical - HITRUST System: Number of users of the system - 500 to 5,500

Change Count: 3

Field	Content
Selection	500 to 5,500500 to 5,500
Order	0022
SelectionLikelihood	0.22.22

Factor View D T O: Technical - HITRUST System: Number of users of the system - Fewer than 500

Change Count: 3

Field	Content
Selection	Fewer than 500Fewer than 500
Order	0011
SelectionLikelihood	0.29.29

Factor View D T O: Technical - HITRUST System: Number of users of the system - Greater than 5,500

Change Count: 3

Field	Content
Selection	Greater than 5,500Greater than 5,500
Order	0033
SelectionLikelihood	0.21.21

Factor View D T O: Technical - HITRUST System: Number of transactions per day - Greater than 85,000

Change Count: 3

Field	Content
Selection	Greater than 85,000Greater than 85,000
Order	0033
SelectionLikelihood	0.22.22

Factor View D T O: Technical - HITRUST System: Number of transactions per day - Fewer than 6,750

Change Count: 3

Field	Content
Selection	Fewer than 6,750Fewer than 6,750

Order	0011
SelectionLikelihood	0.31.31

Factor View D T O: Technical - HITRUST System: Number of transactions per day - 6,750 to 85,000

Change Count: 3

Field	Content
Selection	6,750 to 85,0006,750 to 85,000
Order	0022
SelectionLikelihood	0.19.19

Factor View D T O: Technical - HITRUST System: Number of interfaces - 25 to 75

Change Count: 3

Field	Content
Selection	25 to 7525 to 75
Order	0022
SelectionLikelihood	0.08.08

Factor View D T O: Technical - HITRUST System: Number of interfaces - Fewer than 25

Change Count: 3

Field	Content
Selection	Fewer than 25Fewer than 25
Order	0011
SelectionLikelihood	0.51.51

Factor View D T O: Technical - HITRUST System: Number of interfaces - Greater than 75

Change Count: 3

Field	Content
Selection	Greater than 75Greater than 75
Order	0033
SelectionLikelihood	0.12.12

Factor View D T O: Technical - HITRUST System: Internet - No

Change Count: 3

Field	Content
Selection	NoNo

Order	0011
SelectionLikelihood	0.02.02

Factor View D T O: Technical - HITRUST System: Internet - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.69.69

Factor View D T O: Technical - HITRUST System: Goods Services - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.51.51

Factor View D T O: Technical - HITRUST System: Goods Services - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.20.20

Factor View D T O: Technical - HITRUST System: Fax - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.15.15

Factor View D T O: Technical - HITRUST System: Fax - No

Change Count: 3

Field	Content
Selection	NoNo

Order	0011
SelectionLikelihood	0.56.56

Factor View D T O: Technical - HITRUST System: External Access - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.03.03

Factor View D T O: Technical - HITRUST System: External Access - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.68.68

Factor View D T O: Technical - HITRUST System: Electronic Signatures - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.46.46

Factor View D T O: Technical - HITRUST System: Electronic Signatures - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.25.25

Factor View D T O: Technical - HITRUST System: Dial-Up - No

Change Count: 3

Field	Content
Selection	NoNo

Order	0011
SelectionLikelihood	0.66.66

Factor View D T O: Technical - HITRUST System: Dial-Up - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.05.05

Factor View D T O: Technical - HITRUST System: Development - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.60.60

Factor View D T O: Technical - HITRUST System: Development - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.11.11

Factor View D T O: Technical - HITRUST System: Courier - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.45.45

Factor View D T O: Technical - HITRUST System: Courier - Yes

Change Count: 3

Field	Content
Selection	YesYes

Order	0022
SelectionLikelihood	0.27.27

Factor View D T O: Technical - HITRUST System: Cloud Hosted - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.12.12

Factor View D T O: Technical - HITRUST System: Cloud Hosted - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.59.59

Factor View D T O: Technical - HITRUST System: BYOD - Yes

Change Count: 3

Field	Content
Selection	YesYes
Order	0022
SelectionLikelihood	0.31.31

Factor View D T O: Technical - HITRUST System: BYOD - No

Change Count: 3

Field	Content
Selection	NoNo
Order	0011
SelectionLikelihood	0.40.40

Factor View D T O: Technical - AllSys - Applicable to all systems

Change Count: 3

Field	Content
Selection	Applicable to all systemsApplicable to all systems

Order	00999999
SelectionLikelihood	1.01.00

Factor View D T O: Organizational - AllOrg - Applicable to all Organizations

Change Count: 3

Field	Content
Selection	Applicable to all OrganizationsApplicable to all Organizations
Order	00999999
SelectionLikelihood	1.01.00

Factor View D T O: Organizational - HITRUST Org New: Record Total - Unknown

Change Count: 3

Field	Content
Selection	UnknownUnknown
Order	0011
SelectionLikelihood	0.03.03

Factor View D T O: Organizational - HITRUST Org New: Record Total - Between 10 and 60 Million Records

Change Count: 3

Field	Content
Selection	Between 10 and 60 Million RecordsBetween 10 and 60 Million Records
Order	0033
SelectionLikelihood	0.12.12

Factor View D T O: Organizational - HITRUST Org New: Record Total - Less than 10 Million Records

Change Count: 3

Field	Content
Selection	Less than 10 Million RecordsLess than 10 Million Records
Order	0022
SelectionLikelihood	0.43.43

Factor View D T O: Organizational - HITRUST Org New: Record Total - More than 60 Million Records

Change Count: 3

Field	Content
Selection	More than 60 Million Records More than 60 Million Records
Order	0044
SelectionLikelihood	0.13 .13

Factor View D T O: Organizational - HITRUST Org New: Record Count Annual - More than 725k Records

Change Count: 3

Field	Content
Selection	More than 725k Records More than 725k Records
Order	0044
SelectionLikelihood	0.00 .00

Factor View D T O: Organizational - HITRUST Org New: Record Count Annual - Less than 180k Records

Change Count: 3

Field	Content
Selection	Less than 180k Records Less than 180k Records
Order	0022
SelectionLikelihood	0.00 .00

Factor View D T O: Organizational - HITRUST Org New: Record Count Annual - Between 180k and 725k Records

Change Count: 3

Field	Content
Selection	Between 180k and 725k Records Between 180k and 725k Records
Order	0033
SelectionLikelihood	0.00 .00

Factor View D T O: Organizational - HITRUST Org New: Record Count Annual - Unknown

Change Count: 3

Field	Content
Selection	Unknown Unknown
Order	0011
SelectionLikelihood	0.03 .03

Factor View D T O: Organizational - HITRUST Org New: Physician Encounters - Unknown

Change Count: 3

Field	Content
Selection	Unknown Unknown
Order	0011
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Physician Encounters - Greater than 180k Encounters

Change Count: 3

Field	Content
Selection	Greater than 180k Encounters Greater than 180k Encounters
Order	0044
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Physician Encounters - Fewer than 60k Encounters

Change Count: 3

Field	Content
Selection	Fewer than 60k Encounters Fewer than 60k Encounters
Order	0022
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Physician Encounters - Between 60k to 180k Encounters

Change Count: 3

Field	Content
Selection	Between 60k to 180k Encounters Between 60k to 180k Encounters
Order	0033
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Physician Count - Between 11 and 25 Physicians

Change Count: 3

Field	Content
Selection	Between 11 and 25 Physicians Between 11 and 25 Physicians
Order	0022
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Physician Count - Fewer than 11 Physicians

Change Count: 3

Field	Content
Selection	Fewer than 11 Physicians Fewer than 11 Physicians
Order	0011
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Physician Count - Greater than 25 Physicians

Change Count: 3

Field	Content
Selection	Greater than 25 Physicians Greater than 25 Physicians
Order	0033
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Pharmacy Companies - Greater than 60 million Prescriptions

Change Count: 3

Field	Content
Selection	Greater than 60 million Prescriptions Greater than 60 million Prescriptions
Order	0033
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Pharmacy Companies - Fewer than 10 million Prescriptions

Change Count: 3

Field	Content
Selection	Fewer than 10 million Prescriptions Fewer than 10 million Prescriptions
Order	0011

SelectionLikelihood	0.00.00
---------------------	---------

Factor View D T O: Organizational - HITRUST Org New: Pharmacy Companies - Between 10 million to 60 million Prescriptions

Change Count: 3

Field	Content
Selection	Between 10 million to 60 million Prescriptions Between 10 million to 60 million Prescriptions
Order	0022
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Non-IT Service Provider - Between 25 and 100 Megabytes(MB)

Change Count: 3

Field	Content
Selection	Between 25 and 100 Megabytes(MB) Between 25 and 100 Megabytes(MB)
Order	0022
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Non-IT Service Provider - More than 100 Megabytes(MB)

Change Count: 3

Field	Content
Selection	More than 100 Megabytes(MB) More than 100 Megabytes(MB)
Order	0033
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Non-IT Service Provider - Less than 25 Megabytes(MB)

Change Count: 3

Field	Content
Selection	Less than 25 Megabytes(MB) Less than 25 Megabytes(MB)
Order	0011
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: IT Service Provider - Less than 15 Terabytes(TB)

Change Count: 3

Field	Content
Selection	Less than 15 Terabytes(TB) Less than 15 Terabytes(TB)
Order	0011
SelectionLikelihood	0.01.01

Factor View D T O: Organizational - HITRUST Org New: IT Service Provider - More than 60 Terabytes(TB)

Change Count: 3

Field	Content
Selection	More than 60 Terabytes(TB) More than 60 Terabytes(TB)
Order	0033
SelectionLikelihood	0.01.01

Factor View D T O: Organizational - HITRUST Org New: IT Service Provider - Between 15 and 60 Terabytes(TB)

Change Count: 3

Field	Content
Selection	Between 15 and 60 Terabytes(TB) Between 15 and 60 Terabytes(TB)
Order	0022
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Hospital Admissions - Unknown

Change Count: 3

Field	Content
Selection	Unknown Unknown
Order	0011
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Hospital Admissions - Between 7.5k and 20k Patients

Change Count: 3

Field	Content
Selection	Between 7.5k and 20k Patients Between 7.5k and 20k Patients
Order	0033
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Hospital Admissions - More than 20k Patients

Change Count: 3

Field	Content
Selection	More than 20k Patients More than 20k Patients
Order	0044
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Hospital Admissions - Less than 7.5k Patients

Change Count: 3

Field	Content
Selection	Less than 7.5k Patients Less than 7.5k Patients
Order	0022
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: HIE Transactions - More than 6 Million Transactions

Change Count: 3

Field	Content
Selection	More than 6 Million Transactions More than 6 Million Transactions
Order	0033
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: HIE Transactions - Less than 1 Million Transactions

Change Count: 3

Field	Content
Selection	Less than 1 Million Transactions Less than 1 Million Transactions
Order	0011

SelectionLikelihood	0.00.00
---------------------	---------

Factor View D T O: Organizational - HITRUST Org New: HIE Transactions - Between 1 and 6 Million Transactions

Change Count: 3

Field	Content
Selection	Between 1 and 6 Million Transactions Between 1 and 6 Million Transactions
Order	0022
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Health Plan/Insurance/PBM - Fewer than 1 Million Lives

Change Count: 3

Field	Content
Selection	Fewer than 1 Million Lives Fewer than 1 Million Lives
Order	0011
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Health Plan/Insurance/PBM - Between 1 million to 7.5 Million Lives

Change Count: 3

Field	Content
Selection	Between 1 million to 7.5 Million Lives Between 1 million to 7.5 Million Lives
Order	0022
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Health Plan/Insurance/PBM - Greater than 7.5 Million Lives

Change Count: 3

Field	Content
Selection	Greater than 7.5 Million Lives Greater than 7.5 Million Lives
Order	0033
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Bed - Greater than 750 Beds

Change Count: 3

Field	Content
Selection	Greater than 750 Beds Greater than 750 Beds
Order	0033
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Bed - Between 200 and 750 Beds

Change Count: 3

Field	Content
Selection	Between 200 and 750 Beds Between 200 and 750 Beds
Order	0022
SelectionLikelihood	0.00.00

Factor View D T O: Organizational - HITRUST Org New: Bed - Fewer than 200 Beds

Change Count: 3

Field	Content
Selection	Fewer than 200 Beds Fewer than 200 Beds
Order	0011
SelectionLikelihood	0.00.00