FedRAMP

FedRAMP's Threat to Controls Analysis

Federal Computer Security Managers' Forum

February 2021

GSA

info@fedramp.gov

fedramp.gov

Purpose and Agenda

To gain shared understanding of FedRAMP's Threat-Based Initiative

I. Overview: Threat Based Methodology
II. Applying Threat Based Findings
III. Demo

Why This, Why Now

Enabling Risk Management

Threat Based Authorization Approach

The Challenge:

Authorizing Officials (AOs) have limited information into the current threat landscape which may result in an inherent acceptance of more risk.

The Solution:

FedRAMP partnered with DHS CISA .govCAR to develop a methodology for scoring each FedRAMP security control against the NSA Technical Cyber Threat Framework (NTCTF v2) to determine which security controls and capabilities are most effective to protect, detect, and respond to current prevalent threats.

Benefits:

- Enables agencies, Cloud Service Providers (CSPs), and other industry partners to prioritize security controls that are relevant and effective against the current threat environment.
- Informed, quantitative-based risk management decisions in authorizing information systems for government use.
- Potential for faster authorization timelines by focusing on prioritized security controls.

Why a Threat-Based Approach?

To provide a baseline of threat-based controls that enable CSPs, Agencies, and FedRAMP PMO to quickly produce a real time risk profile for a system.

RISK MANAGEMENT

I. Threat Analysis

Leverages the .govCAR methodology to assign protection values to each security control ranking the controls ability to Protect, Detect, and Respond to a series of threat actions

II. Security Controls Assessment

Decomposition of security controls into control items, to enable a more granular assessment of risk and support automated assessment. Each controls item is assessed and given a value of “satisfied” or “other than satisfied”.

III. Risk Profiling

Utilizes the intersection of the assessment results and the threat analysis to produce an overall risk profile for each security capability and a recommendation which supports the authorization decision

I. Threat Analysis

Threat Analysis

Leverages the .govCAR methodology to assign protection values to each security control ranking the controls ability to Protect, Detect, and Respond to a series of threat actions

Security Controls Scoring

- Controls scoring was completed over 5 scoring sessions each lasting approximately one month.
- Representatives from ***DHS .govCAR, DHS CDM, and FedRAMP*** participated in the scoring sessions that were moderated by VITG, Inc.
- To support scoring of the ***FedRAMP Moderate Baseline*** security controls, each control was decomposed down into its associated control items. Threat scoring was performed at the control item level.
- Data was captured in a series of excel spreadsheets and then inputted into a relational database for further analysis.

Security Control Protection Value

Leveraging a mathematical formula provided by .govCAR and overall protection value (PV) was calculated for each security control based upon the results of the threat analysis.

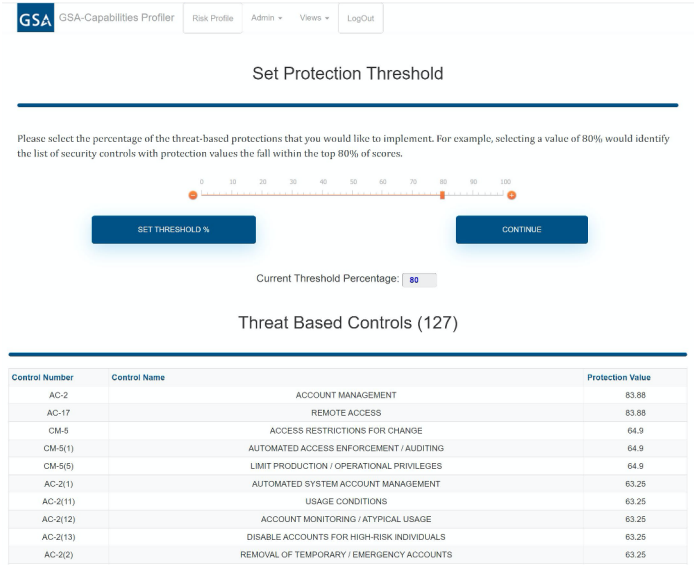
To calculate the overall protection value for each control item, P/D/R functions are weighted as P = .4, D = .3, and R = .3.

The final computation of the control item (PV) is calculated using the following:

$$Protection\ Value\ (PV) = \sum_{TA} TA_{HeatMapValue} * \{.4 * \left(.9P_{S(0,1)} + .6P_{M(0,1)} + .3P_{L(0,1)} + .1P_{A(0,1)}\right) + .3 * \left(.9D_{S(0,1)} + .6D_{M(0,1)} + .3D_{L(0,1)} + .1D_{A(0,1)}\right) + .3 * \left(.9R_{S(0,1)} + .6R_{M(0,1)} + .3R_{L(0,1)} + .1R_{A(0,1)}\right)\}$$

Security Control Prioritization

- Using the established protection values the security controls were ranked in priority order (highest to lowest scores).
- Leveraging the relational database and the threat-based risk profiling application a list of threat-based security controls was produced for various thresholds (i.e. risk tolerances).



Control Number	Control Name	Protection Value
AC-2	ACCOUNT MANAGEMENT	83.88
AC-17	REMOTE ACCESS	83.88
CM-5	ACCESS RESTRICTIONS FOR CHANGE	64.9
CM-5(1)	AUTOMATED ACCESS ENFORCEMENT / AUDITING	64.9
CM-5(5)	LIMIT PRODUCTION / OPERATIONAL PRIVILEGES	64.9
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT	63.25
AC-2(11)	USAGE CONDITIONS	63.25
AC-2(12)	ACCOUNT MONITORING / ATYPICAL USAGE	63.25
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	63.25
AC-2(2)	REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	63.25

II. Security Controls Assessment

Security Controls Assessment

The results of the security controls assessment can be leveraged to produce an implementation value for each control which is weighted based upon the protection values of the related control items. The formula below represents the calculation for control implementation value:

$$Control\ Implementation\ Value = [\sum_{PV} PV_{ControlItems} * (\%control\ items\ implemented)]/PV$$

Account Management (AC-2)		PV	Imp. Status	CI Score	Sub-totals	Imp. Value	%Imp
AC-2(a)	63.25	83.88	1	63.25	47.44	61.19	73%
AC-2(d)	63.25		1	63.25	13.75		
AC-2(e)	63.25		1	63.25			
AC-2(f)	63.25		1	63.25			
AC-2(g)	63.25		1	63.25			
AC-2(h)	63.25		0	0			
AC-2(i)	63.25		0	0			
AC-2(j)	63.25		1	63.25			
AC-2(b)	20.63		1	20.63			
AC-2(c)	20.63		1	20.63			
AC-2(k)	20.63		0	0			

Security Control Implementation Value (AC-2 example)

III. Risk Profiling

To create threat-based risk profile, each of the NIST security controls was mapped to the capabilities listed in NISTIR 8011. The implementation values for each of the NIST 800-53 security controls that was related to a capability were then used to calculate an overall maturity level for each capability.

Example:

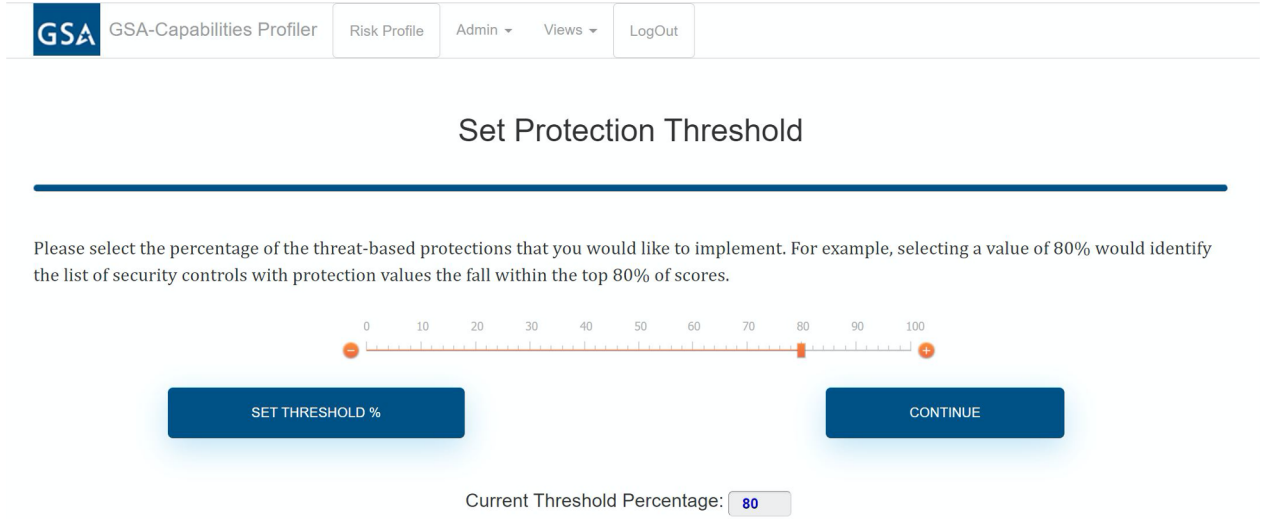
Manage Trust for Person Granted Access (TRUST)		
Control No.	Control Name	% Implemented
AC-2	Account Management	73%
AC-5	Separation of Duties	80%
AC-6	Least Privilege	100%
	Capability Maturity Level:	**84%**

Applications

Opportunity	Impact
Incorporate into Annual Assessment	Enables annual assessments to focus on prioritized threat-based controls.
Assess FedRAMP Tailored Baseline	Simplifies and expedites the process to enter the federal marketplace, equipping systems with the controls that will be most effective against threats.
Agile Authorization Process	Enabled process for information systems can go live once a subset of controls are implemented.
Produce Risk Profile using OSCAL (e.g., SAR, POA&M, CDM sensors)	Enables an automated, near real-time update of the risk profile for an information system to inform a better decision making and enable Ongoing Authorization.
Assist Authorization Decision Making	Provides threat-based data that better informs risk management decisions regarding authorizations.
Prioritize Remediation Efforts	Enables wise resource spending and allocation by allowing the government to attack the most significant problems first.
Identify Desired Future State	Enables strategic planning through the creation of data to assist with road mapping and cost benefit analyses.
Enhance ConMon Activities	Ensures the federal government is focusing resources to achieve the most value as they continuously monitor and improve security of their systems.

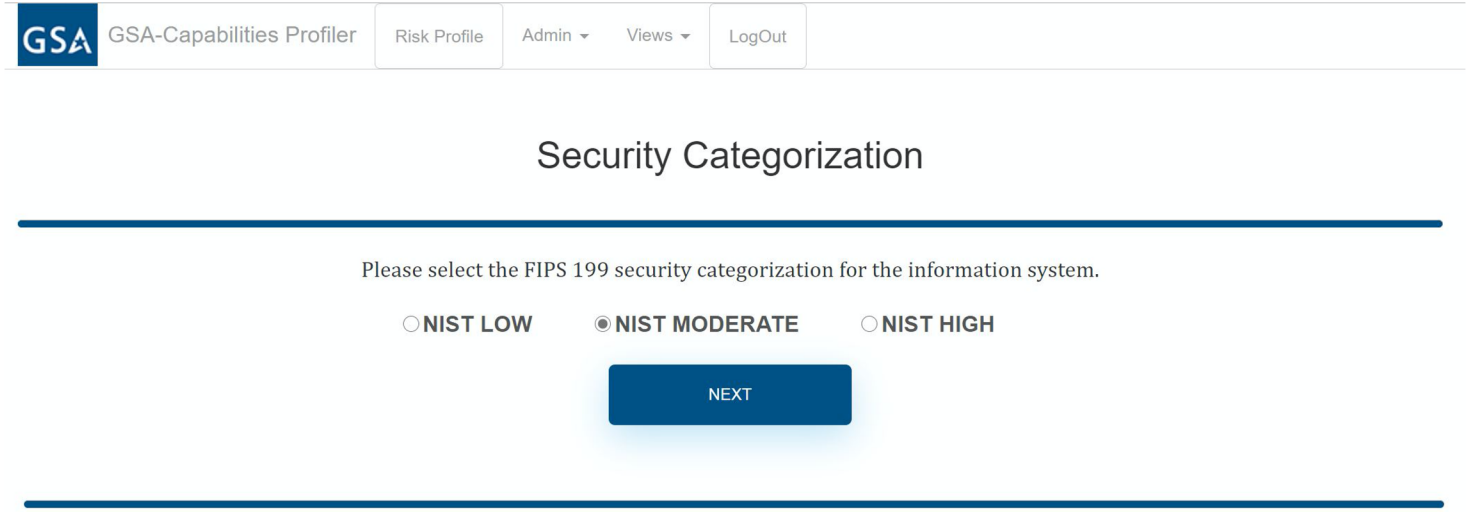
Demo

Demo - Set Protection Threshold

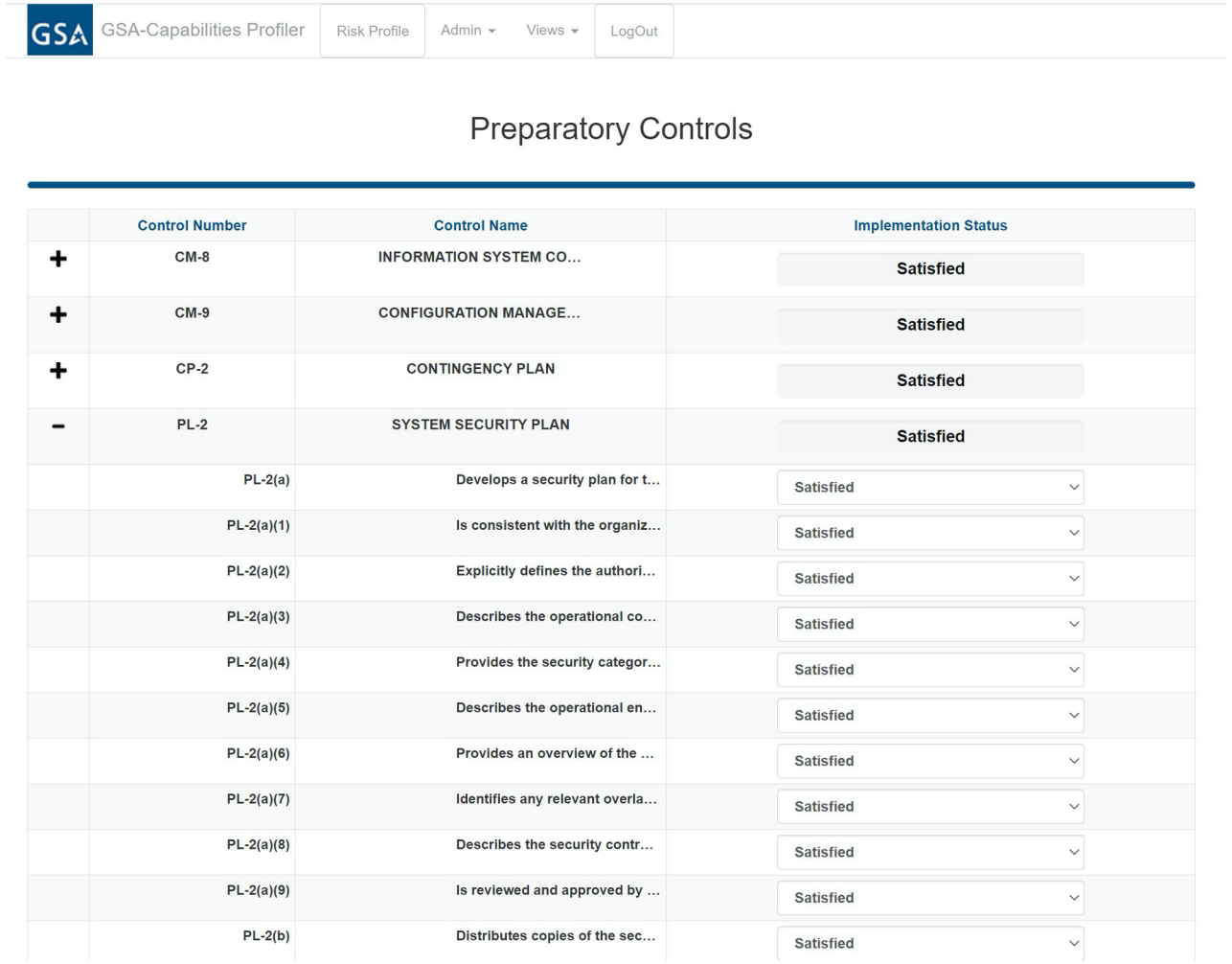


Control Number	Control Name	Protection Value
AC-2	ACCOUNT MANAGEMENT	83.88
AC-17	REMOTE ACCESS	83.88
CM-5	ACCESS RESTRICTIONS FOR CHANGE	64.9
CM-5(1)	AUTOMATED ACCESS ENFORCEMENT / AUDITING	64.9
CM-5(5)	LIMIT PRODUCTION / OPERATIONAL PRIVILEGES	64.9
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT	63.25
AC-2(11)	USAGE CONDITIONS	63.25
AC-2(12)	ACCOUNT MONITORING / ATYPICAL USAGE	63.25
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS	63.25
AC-2(2)	REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS	63.25

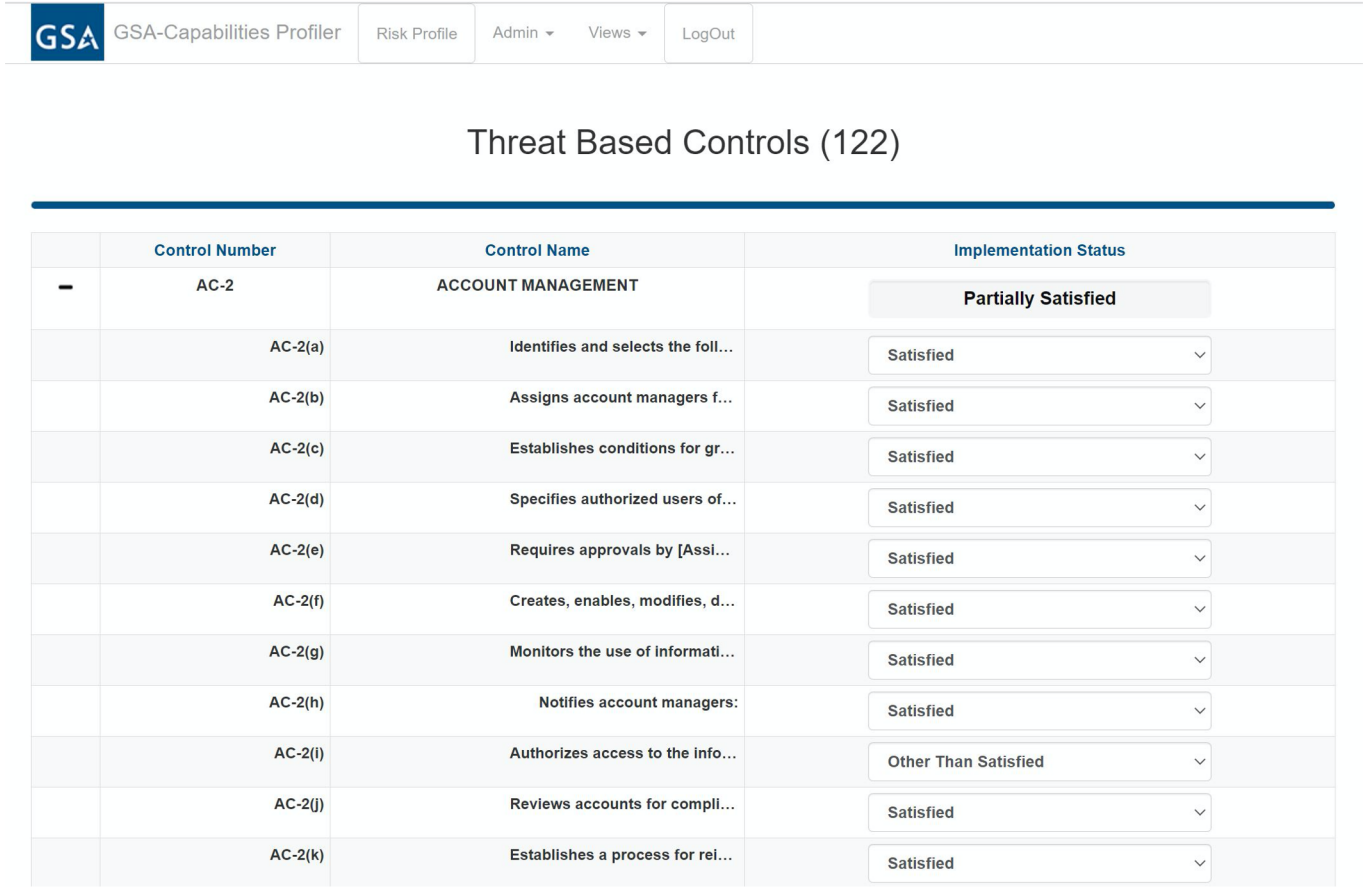
DEMO – Set Categorization



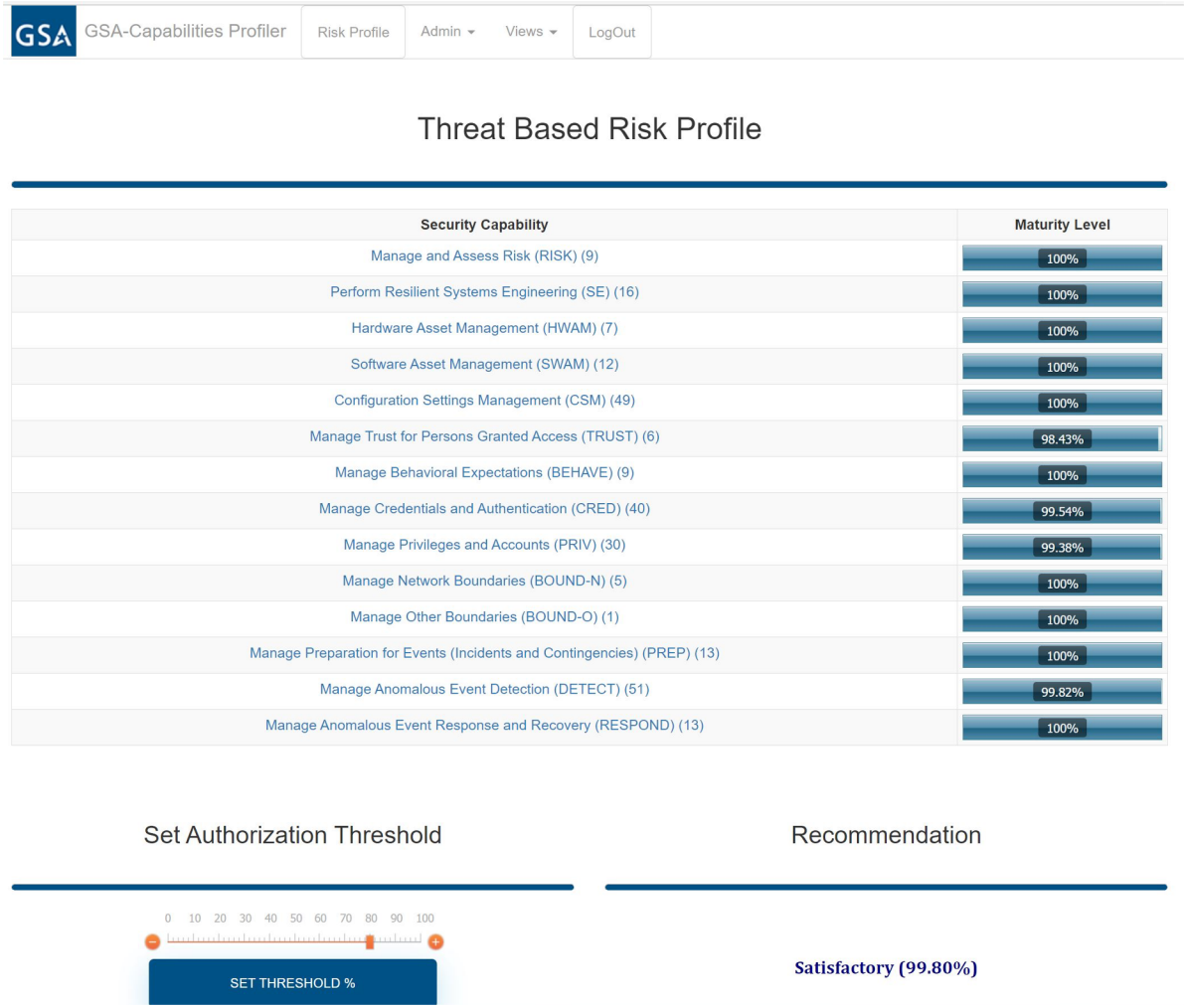
DEMO – Preporatory Controls



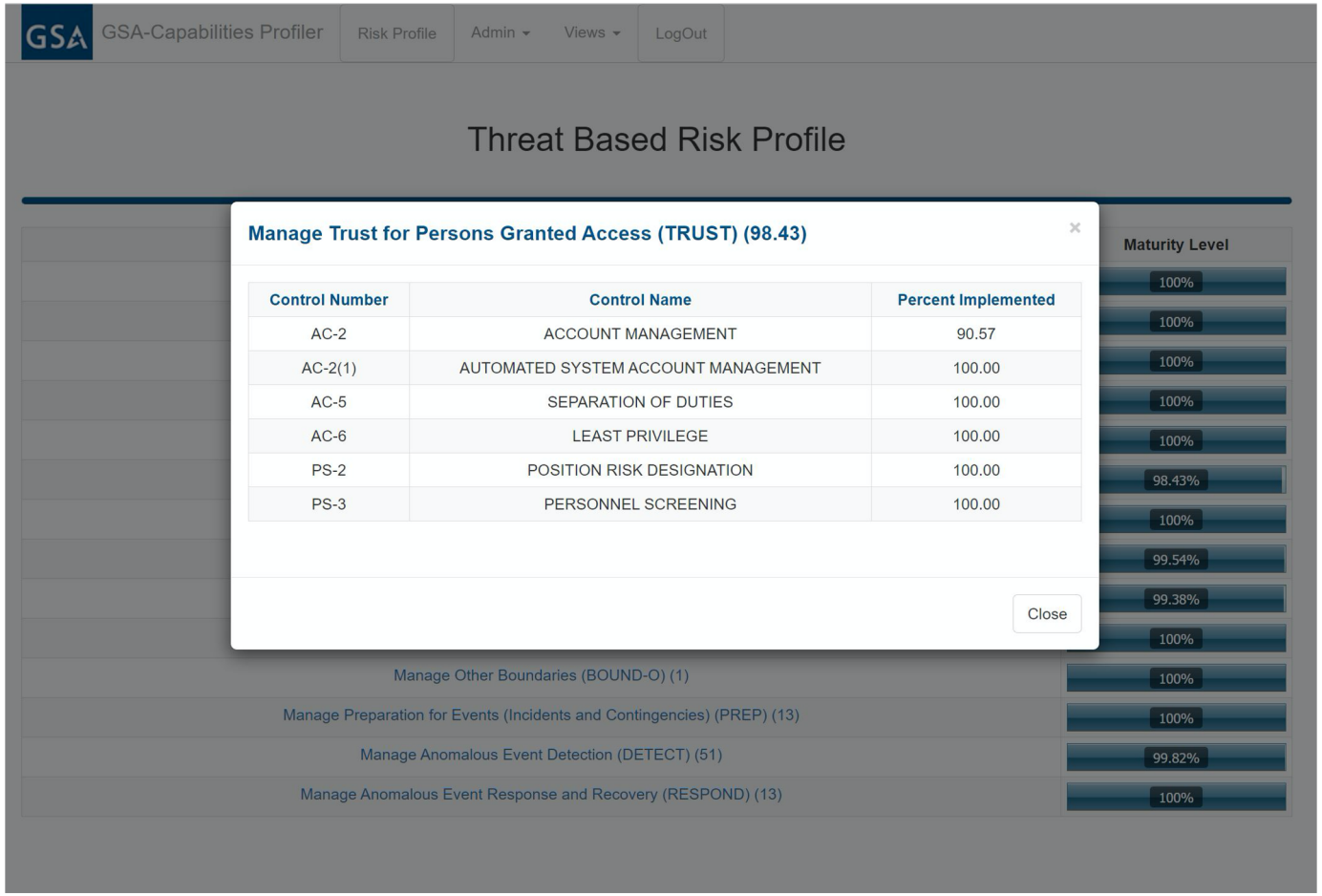
DEMO – Controls Assessment



DEMO – Risk Profile



DEMO – Capability Score



DEMO – Capabilities Mapping

GSA GSA-Capabilities Profiler | Risk Profile | Admin | Views | LogOut

Security Controls to Capabilities Mapping

RISK	SE	HWAM	SWAM	CSM	VULN	TRUST	BEHAVE	CRED	PRIV	BOUND-P	BOUND-N	BOUND-O	PREP	DETECT	RESPOND
AC-1	AC-10	AC-19	CM-2(3)	AC-9	RA-5	AC-2	AC-9	AC-2	AC-2	MA-4	AC-4	AC-17(2)	AT-3	AC-2	AC-1
AT-1	AC-11	AC-19(5)	CM-2(7)	AC-10	RA-5(1)	AC-2(1)	AC-16	AC-2(2)	AC-2(9)	MA-4(1)	AC-17	AC-17(9)	CM-2	AC-2(1)	AU-2
AU-1	AC-11(1)	AC-20	CM-3(1)	AC-11	RA-5(2)	AC-2(9)	AC-16(3)	AC-2(3)	AC-2(10)	MA-5	AC-17(1)	AC-19(5)	CM-2(1)	AC-2(2)	AU-3
CA-1	AC-12	AC-20(2)	CM-3(2)	AC-11(1)	RA-5(3)	AC-5	AT-1	AC-2(4)	AC-3	MA-5(1)	AC-17(3)	SA-4(10)	CM-2(2)	AC-2(3)	AU-3(1)
CA-2(1)	AC-17(9)	CM-2(7)	CM-4	AC-12	RA-5(4)	AC-6	AT-2	AC-2(5)	AC-6	PE-2	AC-17(4)	SC-8	CM-2(3)	AC-2(4)	AU-6
CA-5	AU-6(10)	CM-3	CM-4(1)	AC-14	RA-5(5)	AC-16	AT-2(2)	AC-2(9)	AC-6(1)	PE-2(1)	AC-18	SC-8(1)	CM-2(7)	AC-2(12)	AU-6(1)
CA-5(1)	AU-16	CM-3(1)	CM-5(3)	AC-17(9)		AU-9(4)	AT-3	AC-2(10)	AC-6(2)	PE-3	AC-18(1)	SC-8(2)	CM-6	AC-3	AU-7
CA-6	CA-8	CM-3(2)	CM-7	AC-18(4)		PL-4	AT-4	AC-2(11)	AC-6(3)	PE-3(1)	AC-18(4)	SC-12	CM-6(1)	AC-4	CM-2
CA-7	CA-8(1)	CM-8	CM-7(1)	AU-3		PS-2	AU-1	AC-2(12)	AC-6(5)	PE-4	AC-18(5)	SC-12(1)	CM-6(2)	AC-4(8)	CM-2(1)
CA-7(1)	CM-1	CM-8(1)	CM-7(2)	AU-3(1)		PS-3	AU-2	AC-2(13)	AC-6(9)	PE-5	AC-19	SC-13	CM-8	AC-4(12)	CP-1
CA-9(1)	CM-3	CM-8(2)	CM-7(4)	AU-3(2)		SA-21	AU-5	AC-3(9)	AC-6(10)	PE-6	AC-20	SC-23	CM-8(1)	AC-4(15)	CP-2
CM-1	CM-4(1)	CM-8(3)	CM-7(5)	AU-4			AU-5(1)	AC-6	AC-8	PE-6(1)	AC-20(1)	SC-28	CM-8(2)	AC-4(17)	CP-2(1)
CP-1	CM-5(2)	CM-8(5)	CM-8	AU-5			AU-5(2)	AC-6(3)	AC-16	PE-6(4)	AC-20(2)	SC-28(1)	CM-8(3)	AC-4(18)	CP-2(2)
IA-1	CM-5(3)	IA-4	CM-8(1)	AU-5(1)			AU-6	AC-6(7)	AC-17(4)	PE-8	AC-20(3)	SI-7(6)	CM-8(4)	AC-5	CP-2(3)
IR-1	IR-3	MA-3	CM-8(2)	AU-5(2)			AU-9(4)	AC-6(10)	AU-12(3)	PE-8(1)	CA-3		CM-8(5)	AC-6	CP-2(4)
IR-7	IR-3(2)	MA-3(1)	CM-8(3)	AU-6(1)			AU-12(3)	AC-7	CM-8(4)	PE-9	CA-3(5)		CP-2	AC-6(1)	CP-2(5)
MA-1	IR-5	MA-3(3)	CM-8(4)	AU-6(3)			CM-6(2)	AC-9	IA-1	PE-10	CA-9		CP-2(1)	AC-6(2)	CP-2(8)
MA-2(2)	IR-6	MA-6	CM-8(5)	AU-6(5)			CP-3	AC-9(1)	IA-2	PE-11	IA-2(4)		CP-2(2)	AC-6(7)	CP-4
MA-4(2)	IR-6(1)	MP-6(8)	CM-10	AU-6(6)			IA-2	AC-10	IA-2(1)	PE-11(1)	MA-4		CP-2(3)	AC-6(9)	CP-4(1)
MP-1	IR-10	MP-7(1)	CM-11	AU-7			IA-4	AC-11	IA-2(2)	PE-12	MA-4(3)		CP-2(4)	AC-9	CP-4(2)
PE-1	MA-3	PE-16	MA-3(1)	AU-7(1)			IR-2	AC-11(1)	IA-2(3)	PE-13	SA-9		CP-2(5)	AC-20	CP-4(4)

Visit fedramp.gov to read our full

[Threat Based Risk Profiling Methodology White Paper]

THANK YOU

Learn more at **fedramp.gov**

@FEDRAMP

Questions?