CIMCOR

SOLUTION BRIEF

Centers for Medicare & Medicaid Services Acceptable Risk Safeguards (ARS)

AT A GLANCE

ARS CONTROLS & CIMTRAK ALIGNMENT

» CimTrak aligns and provides direct value to more than 25% of the total ARS controls

EASE OF USE

» Templates and policies readily available to streamline installation and operations

REAL-TIME MONITORING & REMEDIATION

» Mean-Time-To-Identify (MTTI) and Mean-Time-To-Contain (MTTC) security breaches can be measured in seconds with CimTrak

CONTINUOUS COMPLIANCE

» CimTrak provides prescriptive instructions how to fix and correct failed compliance scans

CIMTRAK

Acceptable Risk Safeguards (ARS) 3.1

The Centers for Medicare & Medicaid Services (CMS) Information Security and Privacy Acceptable Risk Safeguards (ARS) provides direction and guidance to CMS and its contractors as the minimum level of acceptable security controls known as the CMS Minimum Security Requirement [CMSR] baselines. The CMSR is based on the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53v4 and a number of other authoritative requirements including:

» Federal Risk and Authorization Management Program (FedRAMP)
» Department of Health and Human Services (HHS) Information Systems Security
» Privacy Policy (IS2P)
» CMS Information Systems Security and Privacy Policy (CMS IS2P2) CMS-CIO-POLSEC-2016-0001
» CMS policies, procedures, and guidance
» And other federal and non-federal guidance and best practices adopted by CMS

ARS Purpose

The overall objective of ARS is to establish minimum standard and set of controls for information security and privacy assurance specific to CMS. These controls were specified and authored by the CMS governing body in addition to other 3rd party organizations that share a knowledge and expertise in information security and privacy assurance. ARS' stated purpose is to provide a "defense-indepth security structure along with a least-privilege" as it complied with CMS IS2P26.

These defined controls in ARS ensure that both CMS and CMS contractors have a minimum standard by which to prioritize and comply in efforts of mitigating the risk though a best practices framework. ARS is by no means an all-inclusive list of controls, but created to highlight people, process and technology requirements of CMS and its operations to safeguard the information which is stores, processes and transmits.
In addition to ARS, CMS systems also need to consider technical requirements:

» CMS Technical Reference Architecture (TRA)
» Various TRA Supplements
» CMS Expedited Life Cycle (XLC)

These documents outline both overall architecture as well as the lifecycle standards required of CMS systems.

The ARS Controls Family

The ARS family of controls contains 26 total control families which make up almost 500 discrete controls. These control families have been selected from domains contained in the NIST 800-52rev4 Special Publication and aligned with 18 of the 20 domains specified in FIPS 200. The addition of 8 non-NIST control families or domains have also been added and encompass control enhancements from HHS IS2P, OMB and other authorities.

NIST 800-53

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Program Management (PM)
- Risk Assessment (RA)
- Security Assessment and Authorization (CA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- System and Services Acquisition (SA)

Non-NIST

- Authority and Purpose (AP)
- Accountability, Audit and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)
- Individual Participation and Redress (IP)
- Security (SE)
- Transparency (TR)
- Use Limitations (UL)

Priority

Of the 480+ controls, each is designated with a priority code to help prioritize the sequencing and implementation of the controls. Priority codes are designated with one of four codes. Priority Code 1 (P1) control is the highest priority followed by P2, P3 and the PO which indicates that the controls is not required.

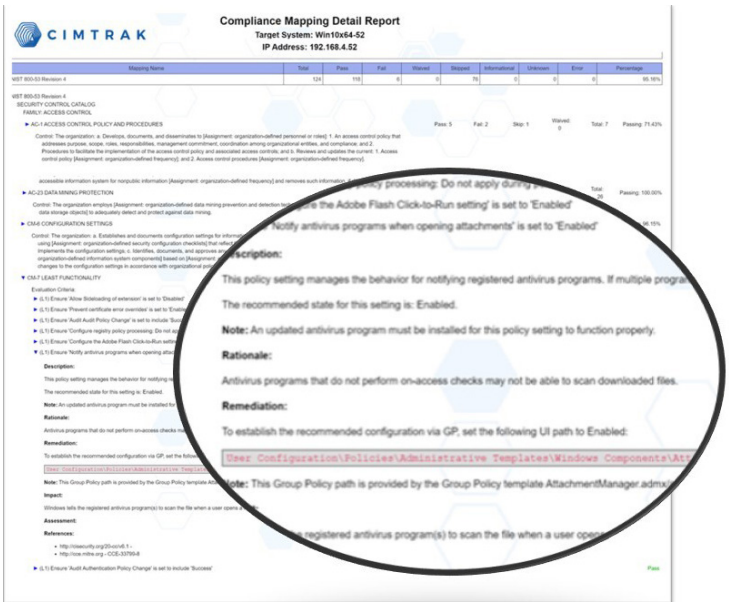
- P1 – 315 Controls
- P2 – 67 Controls
- P3 – 106 Controls
- P0 – 1 Control

How Does CimTrak Align With ARS

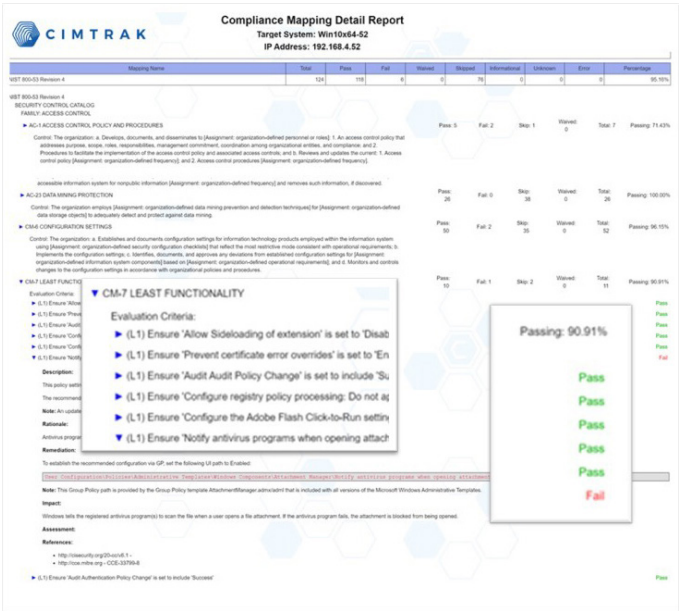
CimTrak aligns with ARS by providing the necessary check and balances of security functionality and security assurance of over a quarter of all the ARS controls. Security functionality refers to the security features, functionality, mechanisms and procedures of information systems and the environments in which they operate. Whereas, security assurance measures the confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system(s).

Of the 26 ARS control families and 489 total controls, CimTrak aligns with 15 families and 134 controls by providing an automated scan or enabling a process, procedure, or policy to assist with the evidence collection to meet the objective of a defined control family. CimTrak refers to this as a crosswalk.

- Access Control (AC)
- Audit and Accountability (AU)
- Configuration Management (CM)
- Contingency Planning (CP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Risk Assessment (RA)
- Security Assessment and Authorization (CA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)
- System and Services Acquisition (SA)
- Accountability, Audit and Risk Management (AR)
- Data Quality and Integrity (DI)
- Data Minimization and Retention (DM)



CimTrak provides the meta-level information associated to a pass or failed compliance scan including description, rationale, impact CIS reference and the expected value. In the event of a failed scan, CimTrak also provides the steps to remediate to a passing status.



CimTrak provides a simple to read and understand summary of each discrete element of a scan that maps to the necessary compliance domain, family and/or control with the ability to drill down into the specific details.

Acceptable Risk Safeguards (ARS) Crosswalk To CimTrak

Access Control (AC)		Accountability, Audit, & Risk Management (AR)		Audit & Accountability (AU)		Assessment, Authorization & Monitoring (CA)		Configuration Management (CM)		Contingency Planning (CP)		Data Quality & Integrity (DI)		Data Minimization & Retention (DM)	
No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak
AC-1		AR-01		AU-1		CA-1		CM-1		CP-1		DI-01		DM-01	
AC-2	✓	AR-02		AU-2	✓	CA-2		CM-2	✓	CP-2		DI-02	✓	DM-02	✓
AC-3	✓	AR-03		AU-3	✓	CA-3		CM-3	✓	CP-3		DI-CMS-01		DM-03	
AC-4		AR-04		AU-4		CA-5		CM-4	✓	CP-4				DM-CMS-01	
AC-5	✓	AR-05		AU-5		CA-6		CM-5	✓	CP-6					
AC-6	✓	AR-06	✓	AU-6	✓	CA-7	✓	CM-6	✓	CP-7					
AC-7		AR-07		AU-7	✓	CA-8		CM-7	✓	CP-8					
AC-8		AR-08	✓	AU-8	✓	CA-9		CM-8	✓	CP-9	✓				
AC-9		AR-CMS-01		AU-9				CM-9		CP-10	✓				
AC-10				AU-10				CM-10							
AC-11				AU-11				CM-11	✓						
AC-12				AU-12											
AC-14				AU-16											
AC-16	✓														
AC-17															
AC-18															
AC-19															
AC-20															
AC-21	✓														
AC-22															
AC-23															
AC-24															
AC-25	✓														

Incident Response (IR)		Maintenance (MA)		Media Protection (MP)		Risk Assessment (RA)		System & Services Acquisition (SA)		System & Communication Protection (SC)		System & Information Integrity (SI)	
No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak	No.	CimTrak
IR-1		MA-1		MP-1		RA-1		SA-1		SC-1		SI-1	
IR-2		MA-2	✓	MP-2	✓	RA-2		SA-2		SC-2	✓	SI-2	✓
IR-3		MA-3	✓	MP-3		RA-3	✓	SA-3	✓	SC-3	✓	SI-3	✓
IR-4	✓	MA-4		MP-4		RA-5	✓	SA-4	✓	SC-4		SI-4	✓
IR-5	✓	MA-5		MP-5				SA-5	✓	SC-5		SI-5	✓
IR-6	✓	MA-6		MP-6				SA-8	✓	SC-7	✓	SI-6	
IR-7	✓			MP-7				SA-9	✓	SC-8	✓	SI-7	✓
IR-8				MP-8				SA-10	✓	SC-10		SI-8	
IR-9				MP-8CMS1				SA-11	✓	SC-12	✓	SI-10	
IR-10								SA-12		SC-13	✓	SI-11	✓
								SA-13		SC-17		SI-12	✓
								SA-15	✓	SC-18		SI-16	
								SA-16		SC-19			
								SA-17		SC-20			
								SA-21		SC-21			
								SA-22		SC-22			
										SC-23			
										SC-24	✓		
										SC-28	✓		
										SC-32			
										SC-39			
										SC-CMS-01			
										SC-CMS-02			

✓ CimTrak Provides a Solution

The chart above is a crosswalk for all CimTrak products if they provide a control, automated scan or enable a process, procedure or policy to assist with the evidence collection to meet the objective of a defined domain, category, control, standard, component or assessment factor.

Supported Platforms

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS: XP, Vista, 7, 8, 10, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise
WINDOWS SERVER: 2003, 2008, 2012, 2016, 2019
LINUX: Amazon, CentOS, ClearOS, Debian, Fedora, Oracle
SUN SOLARIS: x86, SPARC Red Hat, SUSE, Ubuntu, others
MAC: Intel, Power PC
HP-UX: Itanium, PA-RISC
AIX

Windows Parameters Monitored

FILE ADDITIONS, DELETIONS, MODIFICATIONS, AND READS
ATTRIBUTES: compressed, hidden, offline, read-only, archive, reparse point
Creation time, DACL information, Drivers, File opened/read, File Size, File type, Group security information, Installed software, Local groups, Local security policy, Modify time, Registry (keys and values), Services, User groups

UNIX Parameters Monitored

FILE ADDITIONS, DELETIONS, AND MODIFICATIONS
Access Control List, Attributes: read-only, archive, Creation time, File Size, File type, Modify time, User and Group ID

Supported Platforms CimTrak For Network Devices

Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Netgear, NetScreen, Palo Alto, Others

Supported Platforms CimTrak For Databases

Oracle, IBM DB2, Microsoft SQL Server
MySQL PARAMETERS MONITORED, Default rules, Full-text indexes, Functions, Groups, Index definitions, Roles, Stored procedures, Table definitions, Triggers, User defined data types, Users, Views

Supported Hypervisors

Microsoft Hyper-V, VMware ESXi 3x, 4x, 5x, 6x, 7x

Supported Cloud Platforms

Google Cloud, Amazon AWS, Microsoft Azure

Supported Container & Orchestration Integrations

Docker, Docker Enterprise, Kubernetes, Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS)

Supported Ticketing Integrations

CA ServiceDesk, Atlassian Jira, ServiceNow, BMC Remedy

Supported SIEM Integrations

IBM QRadar, McAfee Event Security Manager, Splunk, LogRhythm, Microfocus Arcsight, and others