

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 operation

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 on how to fix and correct failed compliance scans

ACCEPTABLE RISK SAFEGUARDS (ARS) 5.1

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-CIOPOLSEC-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 a 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-in-depth 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 through a best practices framework. ARS is by no means an all-inclusive list of controls, but created to highlight the people, process, and technology requirements of CMS and its operations to safeguard the information which it 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 the 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 has also been added and encompasses 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 are not required.

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

ACCEPTABLE RISK SAFEGUARDS (ARS) CROSSWALK TO CIMTRAK

Access Control (AC)		Awareness & Training (AT)		Audit & Accountability (AU)		Assessment, Authorization & Monitoring (CA)		Configuration Management (CM)		Contingency Planning (CP)		Identification & Authentication (IA)		Incident Response (IR)		Maintenance (MA)		Media Protection (MP)	
#		#		#		#		#		#		#		#		#		#	
AC-1		AT-1		AU-1		CA-1		CM-1		CP-1		IA-1		IR-1		MA-1		MP-1	
AC-2	✓	AT-2		AU-2	✓	CA-2	✓	CM-2	✓	CP-2		IA-2		IR-2		MA-2	✓	MP-2	✓
AC-3	✓	AT-3		AU-3	✓	CA-3		CM-3	✓	CP-3		IA-3		IR-3		MA-3	✓	MP-3	
AC-4		AT-4		AU-4		CA-5		CM-4	✓	CP-4		IA-4		IR-4	✓	MA-4		MP-4	
AC-5	✓	AT-6		AU-5		CA-6		CM-5	✓	CP-6	✓	IA-5		IR-5	✓	MA-5		MP-5	
AC-6	✓			AU-6	✓	CA-7	✓	CM-6	✓	CP-7		IA-6		IR-6	✓	MA-6		MP-6	
AC-7				AU-7	✓	CA-8		CM-7	✓	CP-8		IA-7		IR-7	✓	MA-7		MP-7	
AC-8	✓			AU-8	✓	CA-9		CM-8	✓	CP-9	✓	IA-8		IR-8				MP-8	
AC-9				AU-9	✓			CM-9		CP-10	✓	IA-9		IR-9					
AC-10				AU-10				CM-10		CP-11		IA-10							
AC-11				AU-11				CM-11	✓	CP-12		IA-11							
AC-12				AU-12				CM-12	✓	CP-13	✓	IA-12							
AC-14				AU-13				CM-13											
AC-15				AU-14				CM-14	✓										
AC-16	✓			AU-15															
AC-17				AU-16															
AC-18																			
AC-19																			
AC-20																			
AC-21	✓																		
AC-22																			
AC-23																			
AC-24																			
AC-25	✓																		

ACCEPTABLE RISK SAFEGUARDS (ARS) CROSSWALK TO CIMTRAK

Physical & Environmental Protection (PE)		Planning (PL)		Program Management (PM)		Personnel Security (PS)		Personally Identifiable Information Processing & Transparency (PT)		Risk Assessment (RA)		System & Services Acquisition (SA)		System & Communication Protection (SC)		System & Information Integrity (SI)		Supply Chain Risk Management (SR)	
#		#		#		#		#		#		#		#		#		#	
PE-1		PL-1		PM-1		PS-1		PT-1		RA-1		SA-1		SC-1		SI-1		SR-1	
PE-2		PL-2		PM-2		PS-2		PT-2		RA-2		SA-2		SC-2	✓	SI-2	✓	SR-2	
PE-3		PL-4		PM-3		PS-3		PT-3		RA-3	✓	SA-3	✓	SC-3	✓	SI-3	✓	SR-3	✓
PE-4		PL-7		PM-4		PS-4		PT-4		RA-4		SA-4	✓	SC-4		SI-4	✓	SR-4	✓
PE-5		PL-8		PM-5		PS-5		PT-5		RA-5	✓	SA-5	✓	SC-5		SI-5	✓	SR-5	✓
PE-6		PL-9		PM-6		PS-6		PT-6		RA-6		SA-8	✓	SC-6		SI-6		SR-6	
PE-8		PL-10		PM-7		PS-7		PT-7		RA-7	✓	SA-9	✓	SC-7	✓	SI-7	✓	SR-7	
PE-9		PL-11		PM-8		PS-8		PT-8		RA-8		SA-10	✓	SC-8	✓	SI-8		SR-8	
PE-10				PM-9		PS-9				RA-9		SA-11	✓	SC-9	✓	SI-10		SR-9	✓
PE-11				PM-10						RA-10	✓	SA-15	✓	SC-10		SI-11	✓	SR-10	✓
PE-12				PM-11								SA-16		SC-11	✓	SI-12	✓	SR-11	✓
PE-13				PM-12								SA-17		SC-12		SI-13		SR-12	
PE-14				PM-13								SA-20	✓	SC-13		SI-14	✓		
PE-15				PM-14								SA-21		SC-14		SI-15	✓		
PE-16				PM-15								SA-22		SC-15	✓	SI-16			
PE-17				PM-16								SA-23		SC-16	✓	SI-17			
PE-18				PM-17										SC-17	✓	SI-18			
PE-19				PM-18										SC-18	✓	SI-19			
PE-20				PM-19										SC-19	✓	SI-20			
PE-21				PM-20										SC-20	✓	SI-21	✓		
PE-22				PM-21										SC-21	✓	SI-22			
PE-23				PM-22										SC-22	✓	SI-23			
				PM-23										SC-23	✓				
				PM-24										SC-24	✓				
				PM-25										SC-25	✓				
				PM-26										SC-26	✓				
				PM-27										SC-27	✓				
				PM-28										SC-28	✓				
				PM-29										SC-29	✓				
				PM-30										SC-30	✓				
				PM-31										SC-31	✓				
				PM-32										SC-32	✓				
														SC-33	✓				
														SC-34	✓				
														SC-35	✓				
														SC-36	✓				
														SC-37	✓				
														SC-38	✓				
														SC-39	✓				
														SC-40	✓				
														SC-41	✓				
														SC-42	✓				
														SC-43	✓				
														SC-44	✓				
														SC-45	✓				
														SC-46	✓				
														SC-47	✓				
														SC-48	✓				
														SC-49	✓				
														SC-50	✓				
														SC-51	✓				

SUPPORTED PLATFORMS

CimTrak for Servers, Critical Workstations & POS Systems

WINDOWS XP, Vista, 7, 8, 10, 11, Embedded for Point of Service (WEPOS), POSReady, Windows 10 IoT Enterprise, Windows 11 IoT Enterprise

WINDOWS SERVER 2003, 2008, 2012, 2016, 2019, 2022

LINUX Alma, Amazon, ARM, CentOS, ClearOS, Debian, Fedora, Oracle, Red Hat, Rocky, SUSE, Ubuntu, others

FreeBSD 12, 13

SUN SOLARIS x86/SPARC

MacOS 5, 6, 7, 8, 9, 10, 11

HP-UX Itanium, PA-RISC

AIX 6.1, 7.1, 7.2, 7.3

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 BENCHMARKS

ALIBABA

ALMA

AMAZON ELASTIC KUBERNETES

AMAZON LINUX

APACHE

APPLE MAC OS

AZURE

CENTOS

CISCO Firewall, IOS

DEBIAN

DISTRIBUTION INDEPENDENT

FEDORA

GOOGLE Chrome, Container, Kubernetes

IBM

KUBERNETES

MICROSOFT Access, Edge, Excel,

IIS, Intune, Office, PowerPoint, SharePoint, SQL, Windows, Windows Server, Word

MONGODB

NGINX

ORACLE Cloud, Database, Linux, MySQL

PALO ALTO

POSTGRESQL

RED HAT

RHEL8

ROCKY

ROS

SUSE

UBUNTU LXCD, Linux

VMWARE

Supported Platforms CimTrak For Network Devices

Arista, Aruba, Cisco, Check Point, Extreme, F5, Fortinet, HP, Juniper, Palo Alto, Sophos, others

Supported Platforms CimTrak For Databases

IBM DB2, Microsoft SQL Server, MySQL, Oracle

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

Amazon AWS, Google Cloud, Microsoft Azure

Supported Container & Orchestration Integrations

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

Supported Ticketing Integrations

Atlassian Jira, BMC Remedy, CA ServiceDesk, ServiceNow

Supported SIEM Integrations

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

Supported Under CimTrak's Trusted File Registry™

CentOS 7, Microsoft Windows 7, 8, 8.1, 10, 11, XP, 2003, 2008, 2012, 2016, 2019, 2022, Oracle Linux 7, Redhat Enterprise Linux 7

