Unit #5b

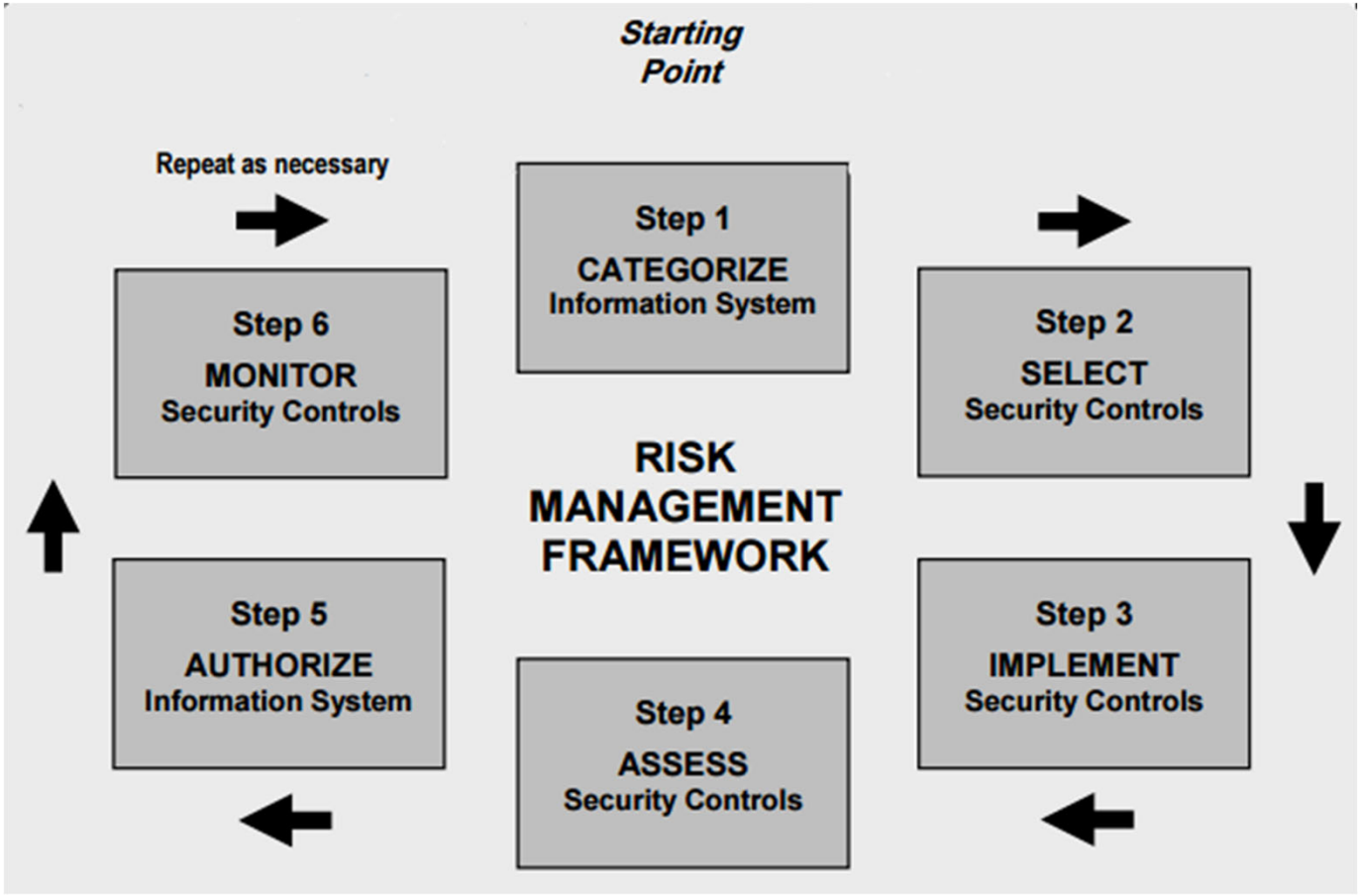
MIS5214

Host Hardening

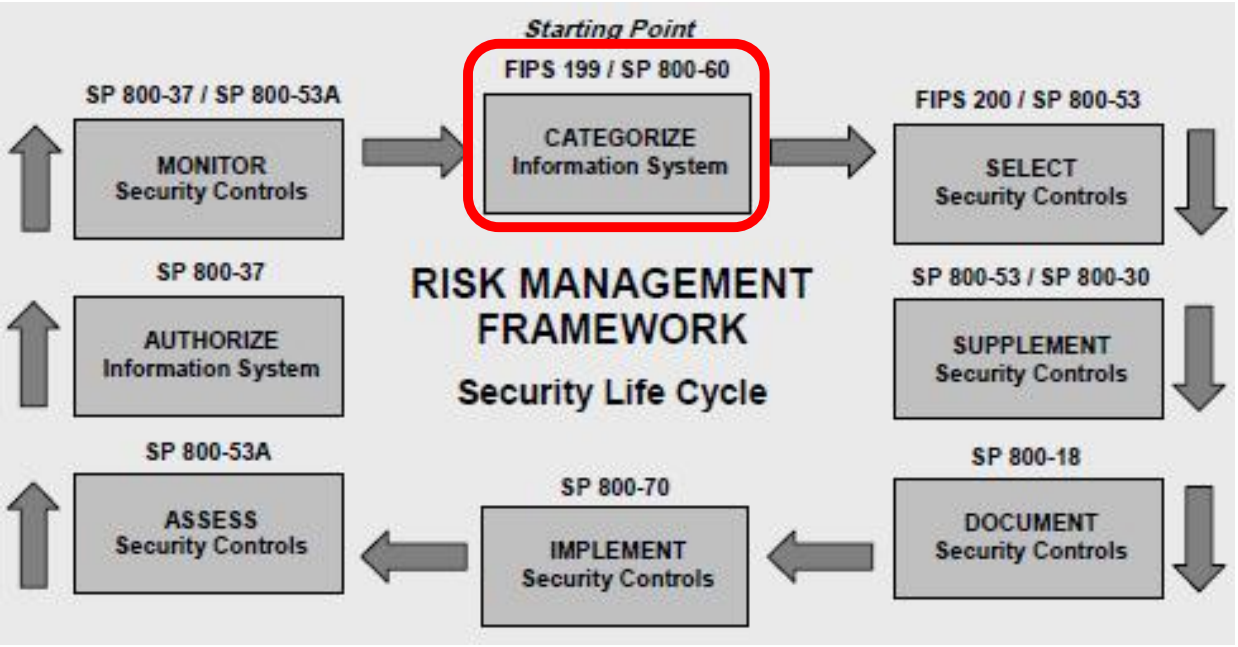
Agenda

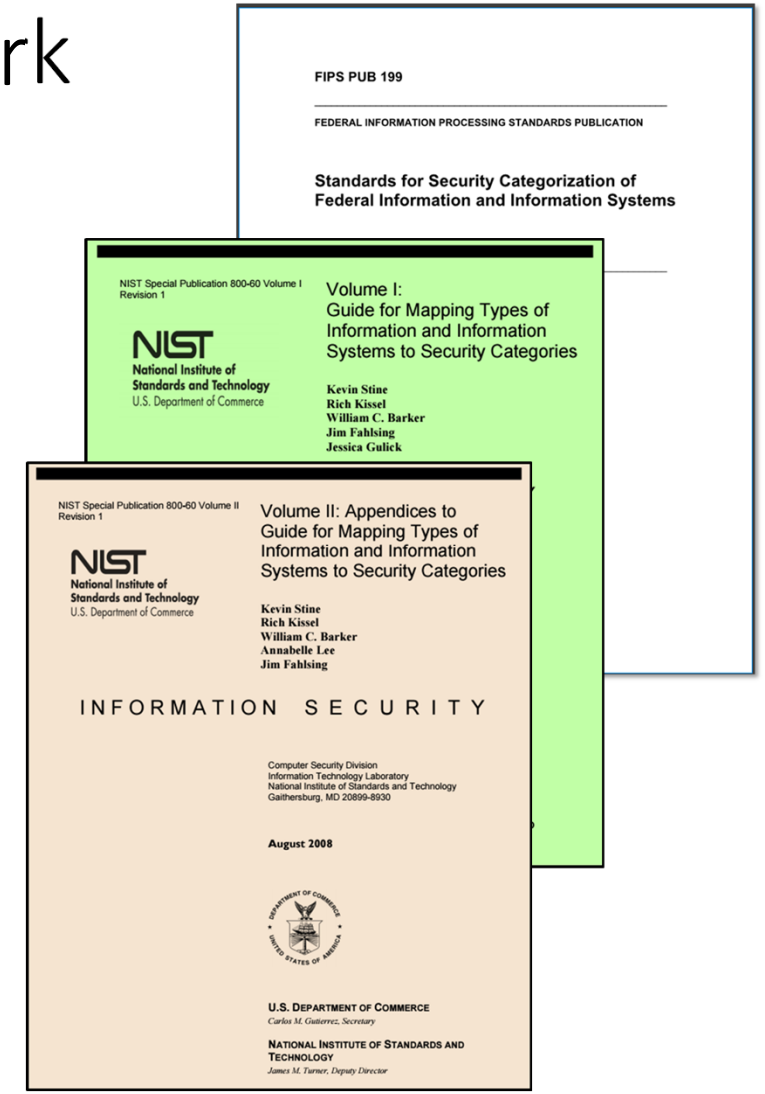
- Risk Management Framework – A quick review…
- Implementing controls – Host hardening…
  - Security configuration checklist (with STIG Viewer)
- SCAP - Security Content Automation Protocol
- System Security Plan's Section 13
  - Select 1 control family to fill out for your information system
- System Security Plan's Section 8
  - Information System Type
- Team Project - SSP draft development…

NIST Risk Management Framework

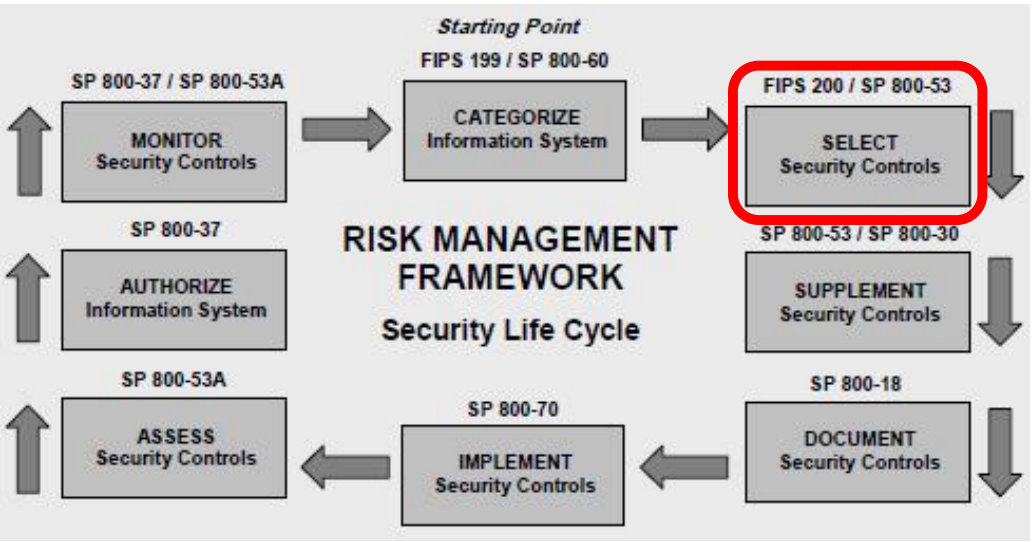


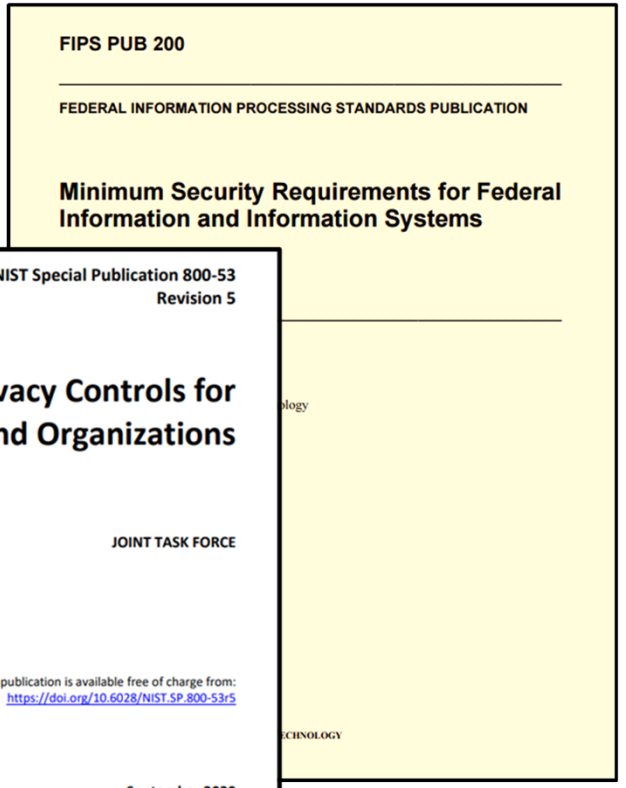
NIST Risk Management Framework





NIST Risk Management Framework

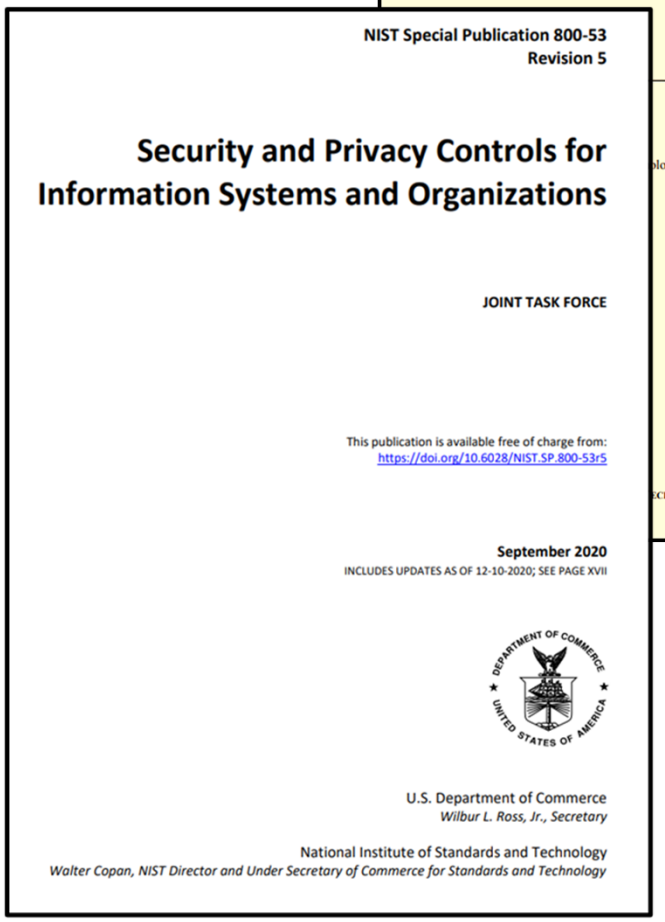




FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

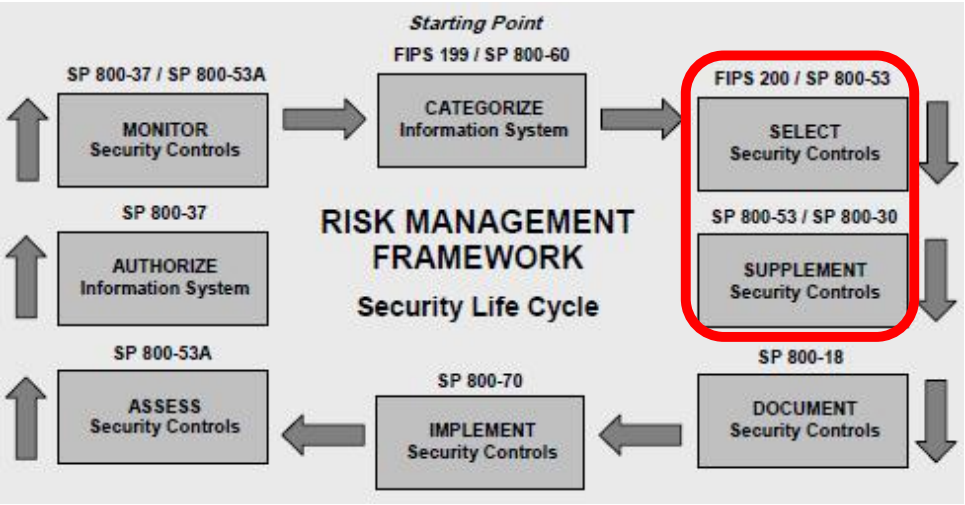
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

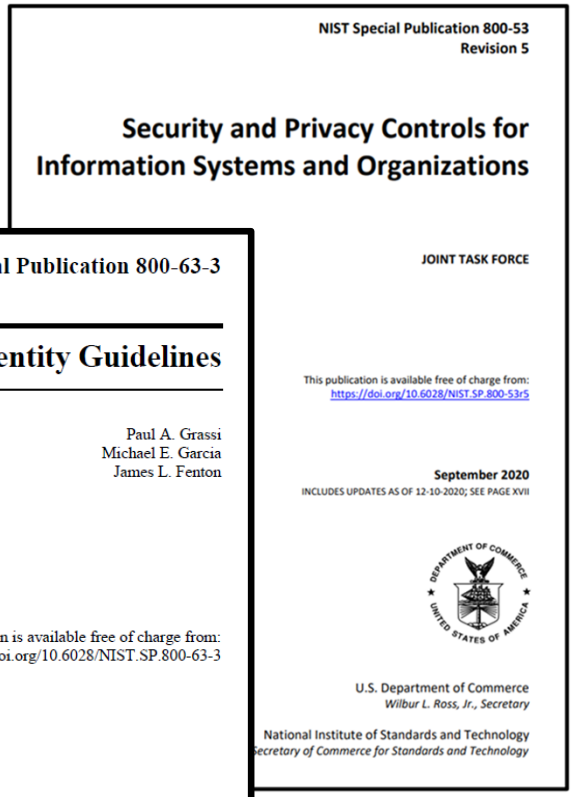
September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Risk Management Framework





NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for
Information Systems and Organizations

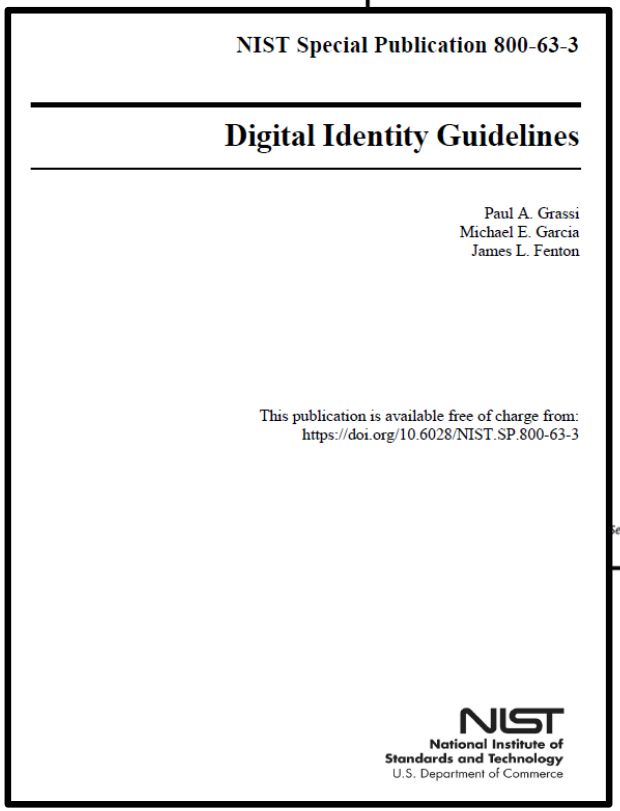
JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Secretary of Commerce for Standards and Technology



NIST Special Publication 800-63-3

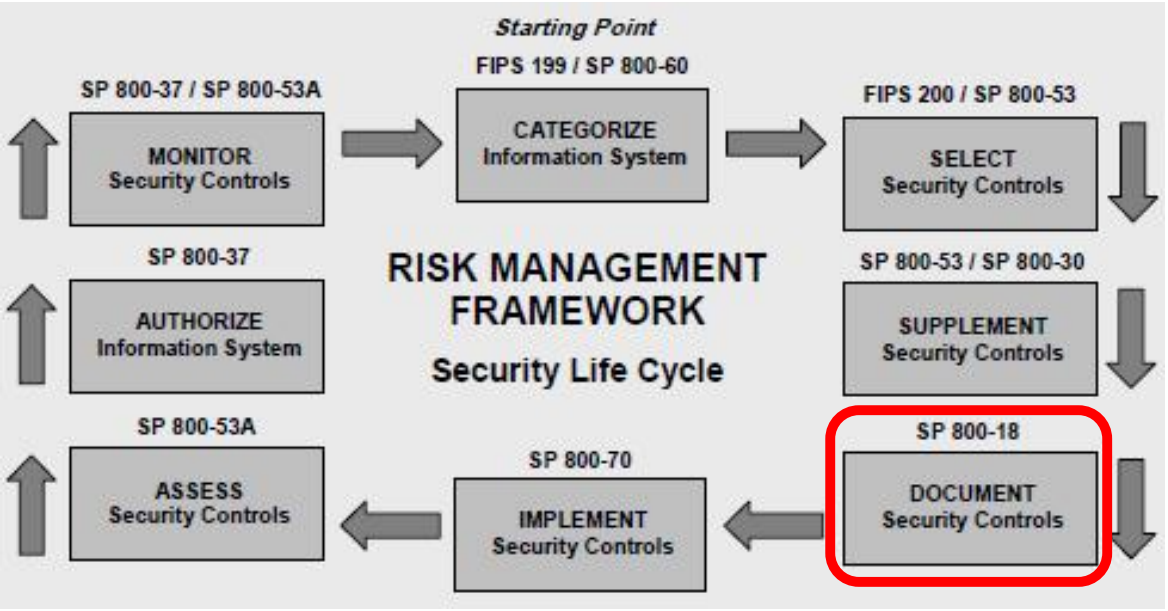
Digital Identity Guidelines

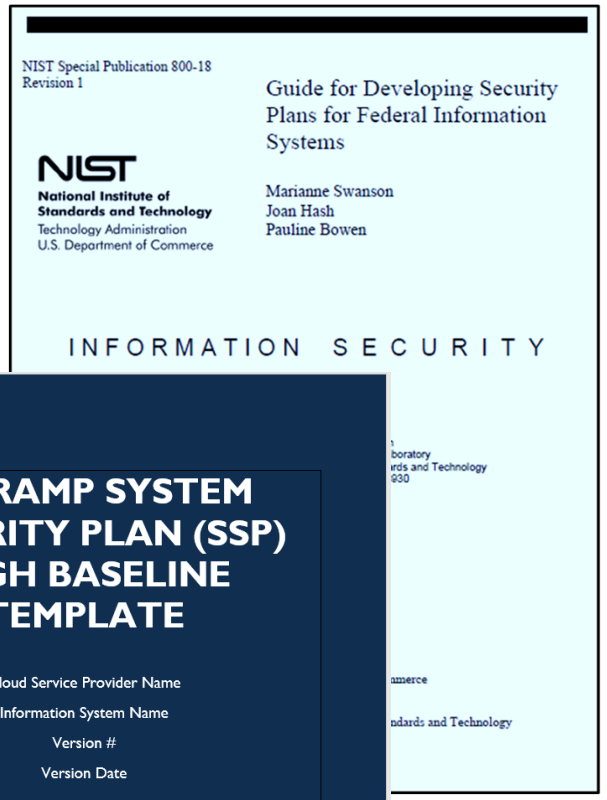
Paul A. Grassi
Michael E. Garcia
James L. Fenton

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

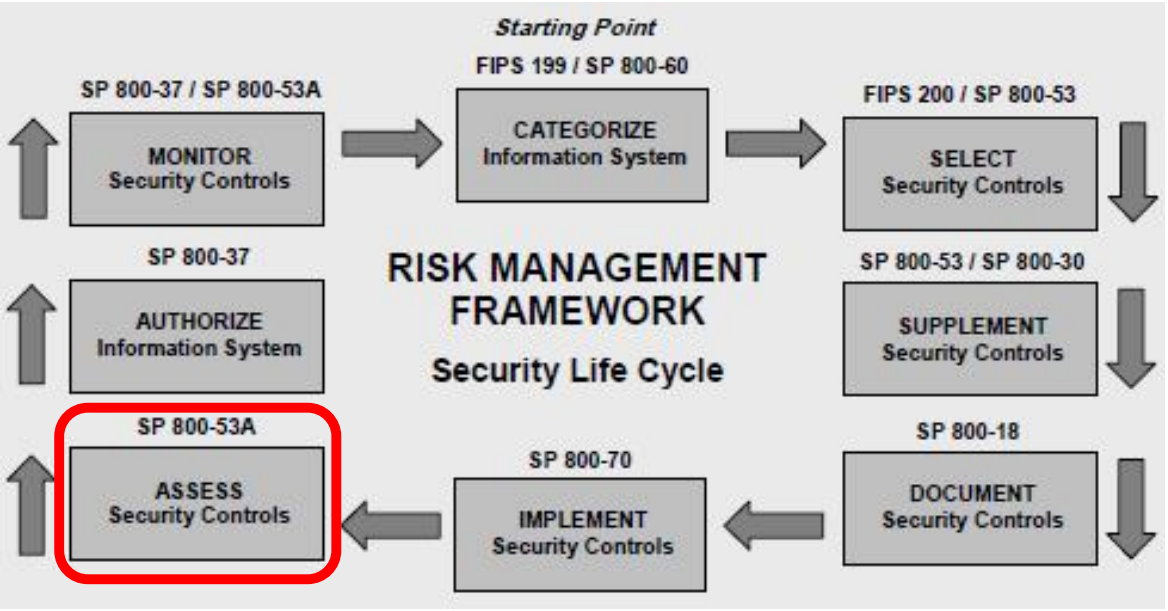
NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

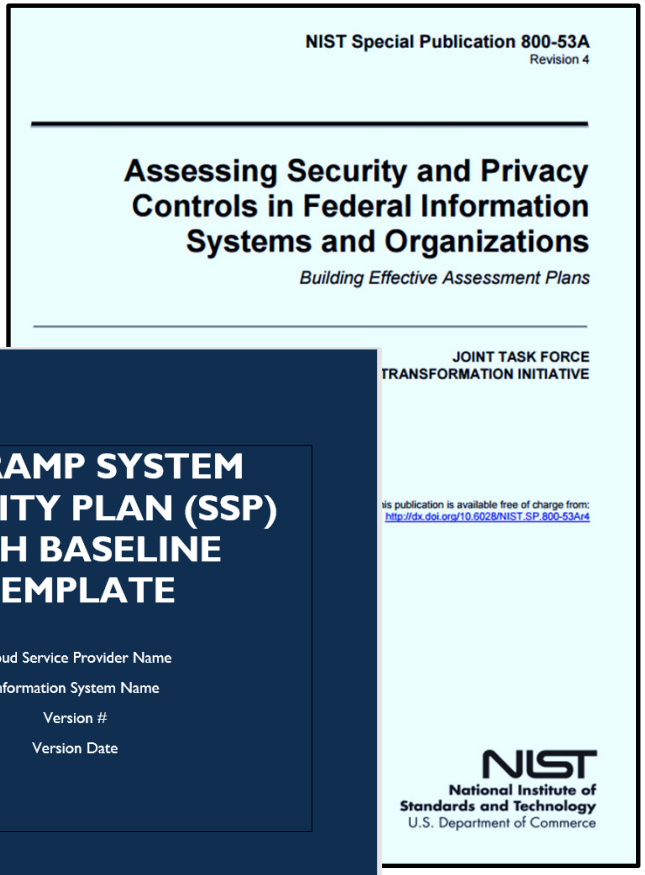
NIST Risk Management Framework





NIST Risk Management Framework




NIST Special Publication 800-53A
Revision 4

Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Building Effective Assessment Plans

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

is publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53Ar4

NIST
National Institute of Standards and Technology
U.S. Department of Commerce


FEDRAMP SYSTEM SECURITY PLAN (SSP) HIGH BASELINE TEMPLATE

Cloud Service Provider Name

Information System Name

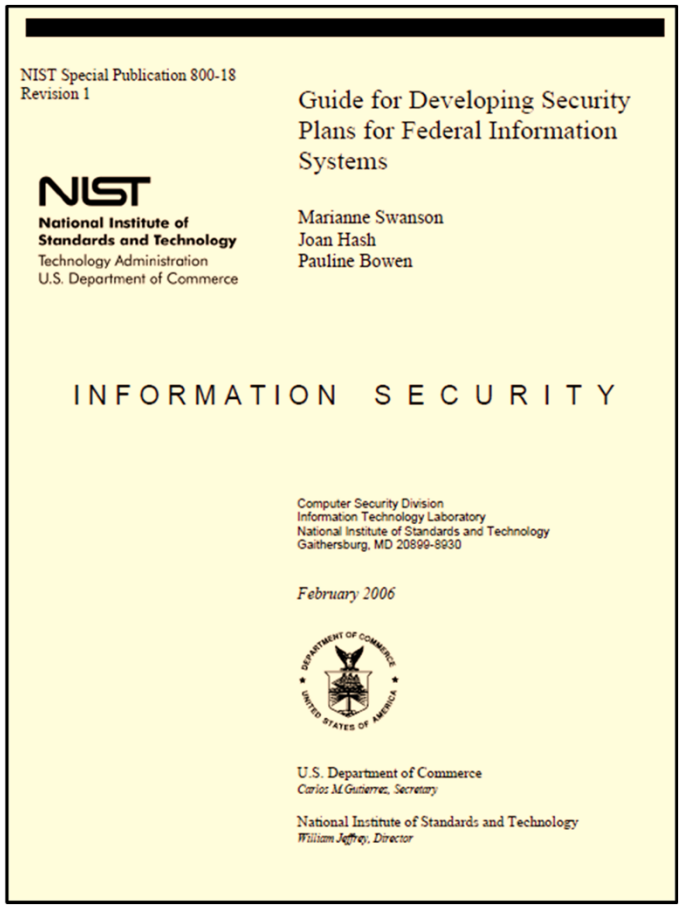
Version #

Version Date

FedRAMP

CONTROLLED UNCLASSIFIED INFORMATION

Which controls aid in Host Hardening… ?



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

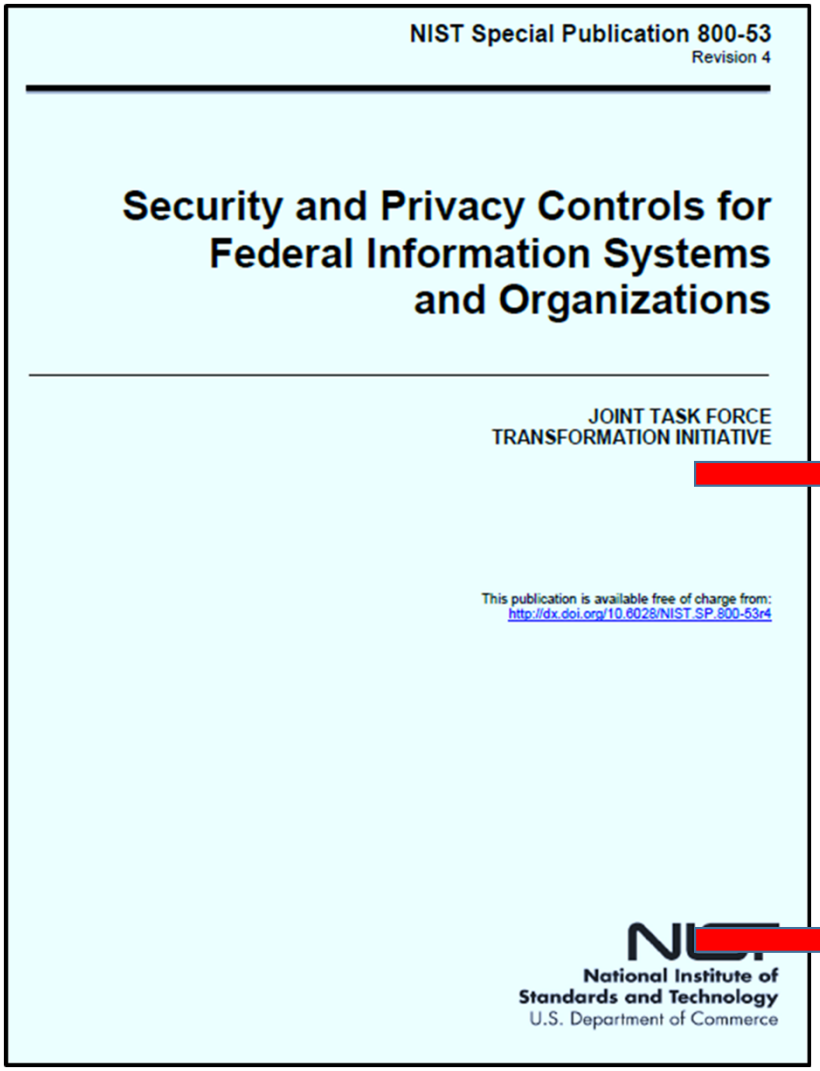
February 2006

U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

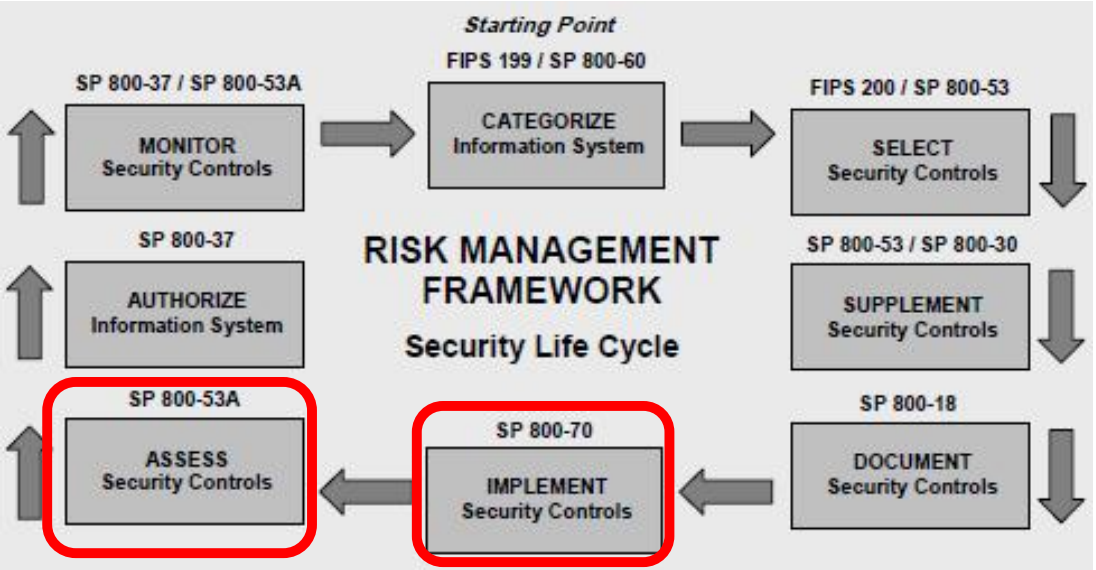
National Institute of Standards and Technology
William Jeffrey, Director

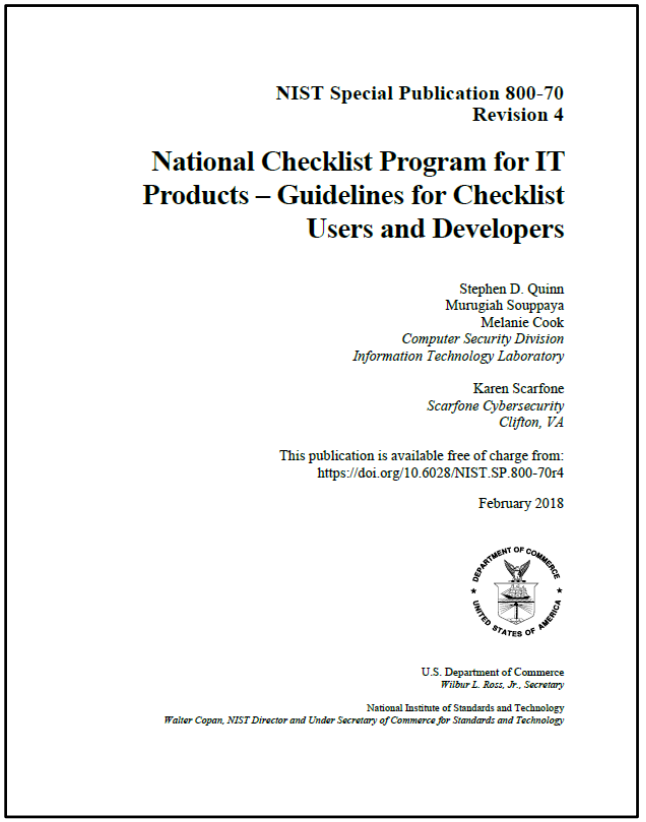
CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier



CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Configuration Management					
CM-1	Configuration Management Policy and Procedures	P1	CM-1	CM-1	CM-1
CM-2	Baseline Configuration	P1	CM-2	CM-2 (1) (3) (7)	CM-2 (1) (2) (3) (7)
CM-3	Configuration Change Control	P1	Not Selected	CM-3 (2)	CM-3 (1) (2)
CM-4	Security Impact Analysis	P2	CM-4	CM-4	CM-4 (1)
CM-5	Access Restrictions for Change	P1	Not Selected	CM-5	CM-5 (1) (2) (3)
CM-6	Configuration Settings	P1	CM-6	CM-6	CM-6 (1) (2)
CM-7	Least Functionality	P1	CM-7	CM-7 (1) (2) (4)	CM-7 (1) (2) (5)
CM-8	Information System Component Inventory	P1	CM-8	CM-8 (1) (3) (5)	CM-8 (1) (2) (3) (4) (5)
CM-9	Configuration Management Plan	P1	Not Selected	CM-9	CM-9
CM-10	Software Usage Restrictions	P2	CM-10	CM-10	CM-10
CM-11	User-Installed Software	P1	CM-11	CM-11	CM-11
Risk Assessment					
RA-1	Risk Assessment Policy and Procedures	P1	RA-1	RA-1	RA-1
RA-2	Security Categorization	P1	RA-2	RA-2	RA-2
RA-3	Risk Assessment	P1	RA-3	RA-3	RA-3
RA-4	**Withdrawn**	---	---	---	---
RA-5	Vulnerability Scanning	P1	RA-5	RA-5 (1) (2) (5)	RA-5 (1) (2) (4) (5)





NIST Special Publication 800-70
Revision 4

National Checklist Program for IT Products – Guidelines for Checklist Users and Developers

Stephen D. Quinn
Murugiah Souppaya
Melanie Cook
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-70r4

February 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

A security configuration checklist is a document containing instructions or procedures for:

- Configuring an information technology (IT) product to an operational environment
- Verifying that the product has been configured properly
- Identifying unauthorized changes to the product

Checklists can help you:

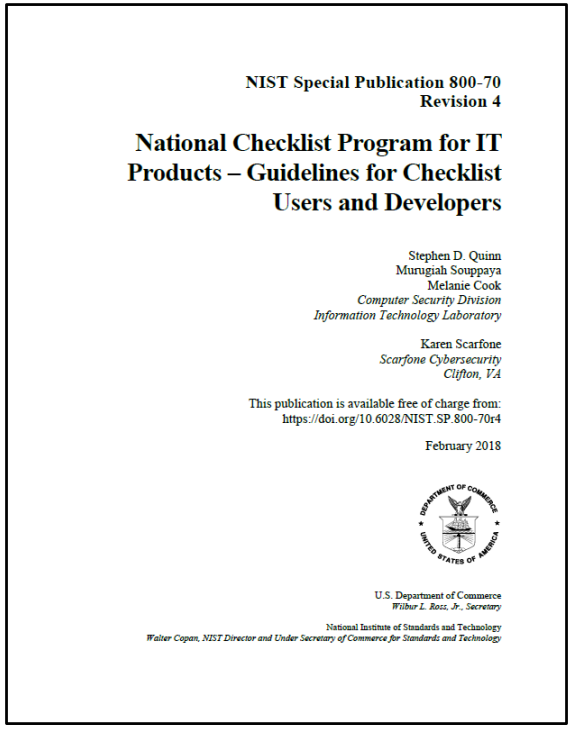
- Minimize the attack surface
- Reduce vulnerabilities
- Lessen the impact of successful attacks
- Identify changes that might otherwise go undetected

Two types of checklists

- **Non-Automated**
  - Designed to be used manually, such as written instructions that describe the steps an administrator should take to secure a system or to verify its security settings
- **Automated**
  - Used through one or more tools that automatically alter or verify settings based on the contents of the checklist
  - Many checklists are written in Extensible Markup Language (XML), and there are special tools that can use the contents of the XML files to check and alter system settings
    - Security Content Automation Protocol (SCAP) is a common example used to express checklist content in a standardized way that can be processed by tools that support SCAP

Security Configuration Checklist

- There is no checklist that can make a system or product 100 percent secure
- Using checklists does not eliminate the need for ongoing security maintenance, such as patch installation
- Using checklists for hardening systems against software flaws (e.g., by applying patches and eliminating unnecessary functionality) and configuring systems securely will typically:
  - Reduce the number of ways in which systems can be attacked
  - Result in greater product security and protection from threats
  - Help verify the configuration of some types of security controls for system assessments



NIST Special Publication 800-70
Revision 4

National Checklist Program for IT Products – Guidelines for Checklist Users and Developers

Stephen D. Quinn
Murugiah Souppaya
Melanie Cook
Computer Security Division
Information Technology Laboratory

Karen Scarfone
Scarfone Cybersecurity
Clifton, VA

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-70r4

February 2018

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

ISACA is a source of many audit control checklists

AUDIT PROGRAM

UNIX/LINUX Operating System Security Audit Program

Objective—The objective of the UNIX/LINUX Audit program is to provide management with an independent assessment relating to the effectiveness of configuration and security of the UNIX/LINUX operations systems...

FREE to ISACA Members
Not a Member? Join Now

AUDIT PROGRAM

Windows Active Directory Audit Program

Objective—The Active Directory audit review will: Provide management with an evaluation of the Active Directory implementation and management security design effectiveness Provide management with an independent...

FREE to ISACA Members
Not a Member? Join Now

AUDIT PROGRAM

Network Perimeter Security Audit Program

Objective—The objectives of the network perimeter security audit review are to:Provide management with an independent assessment relating to the effectiveness of the network perimeter security and its alignment with...

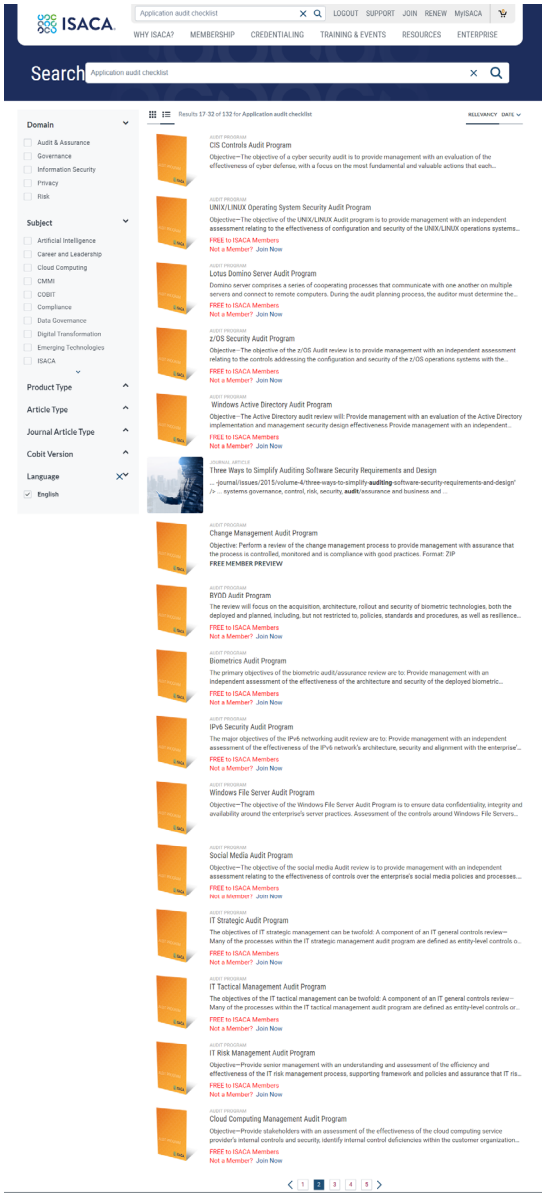
FREE MEMBER PREVIEW

AUDIT PROGRAM

Secure Shell Protocol (SSH) Audit Program

Objective—Provides enterprises with a means to assess the effectiveness of their use of the SSH protocol, including key management and applicable SSH controls. Scope—The use of the Secure Shell (SSH) protocol...

FREE to ISACA Members
Not a Member? Join Now



UNIX/LINUX Operating System Security Audit Program

Audit Program

Digital materials can be accessed from the Downloaded Materials tab of your *MyISACA* account.

Pages	Date Published	Status
55	2009	Available

Language	Format
English	Digital

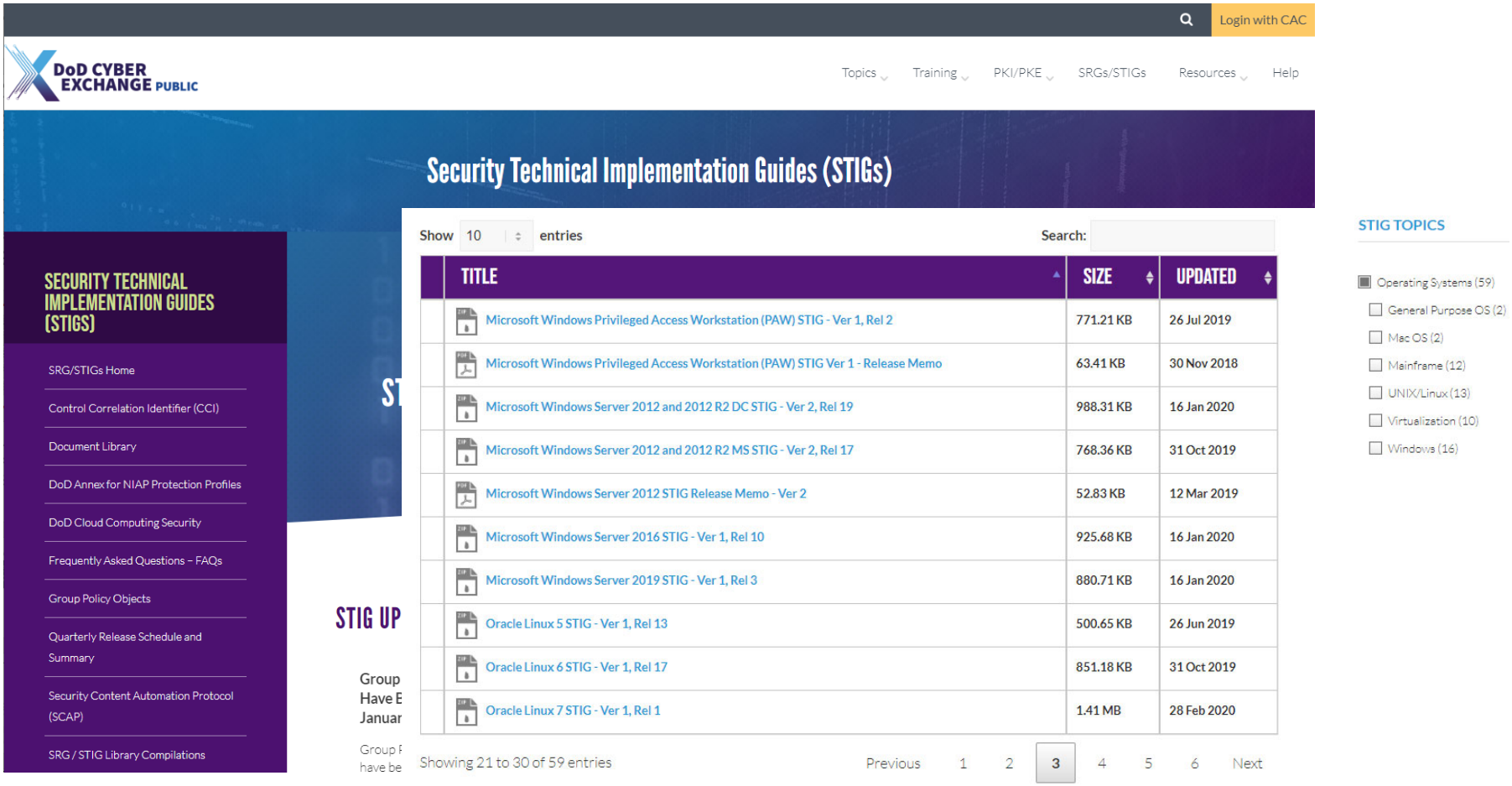
UNIX/LINUX Operating System Security Audit/Assurance Program

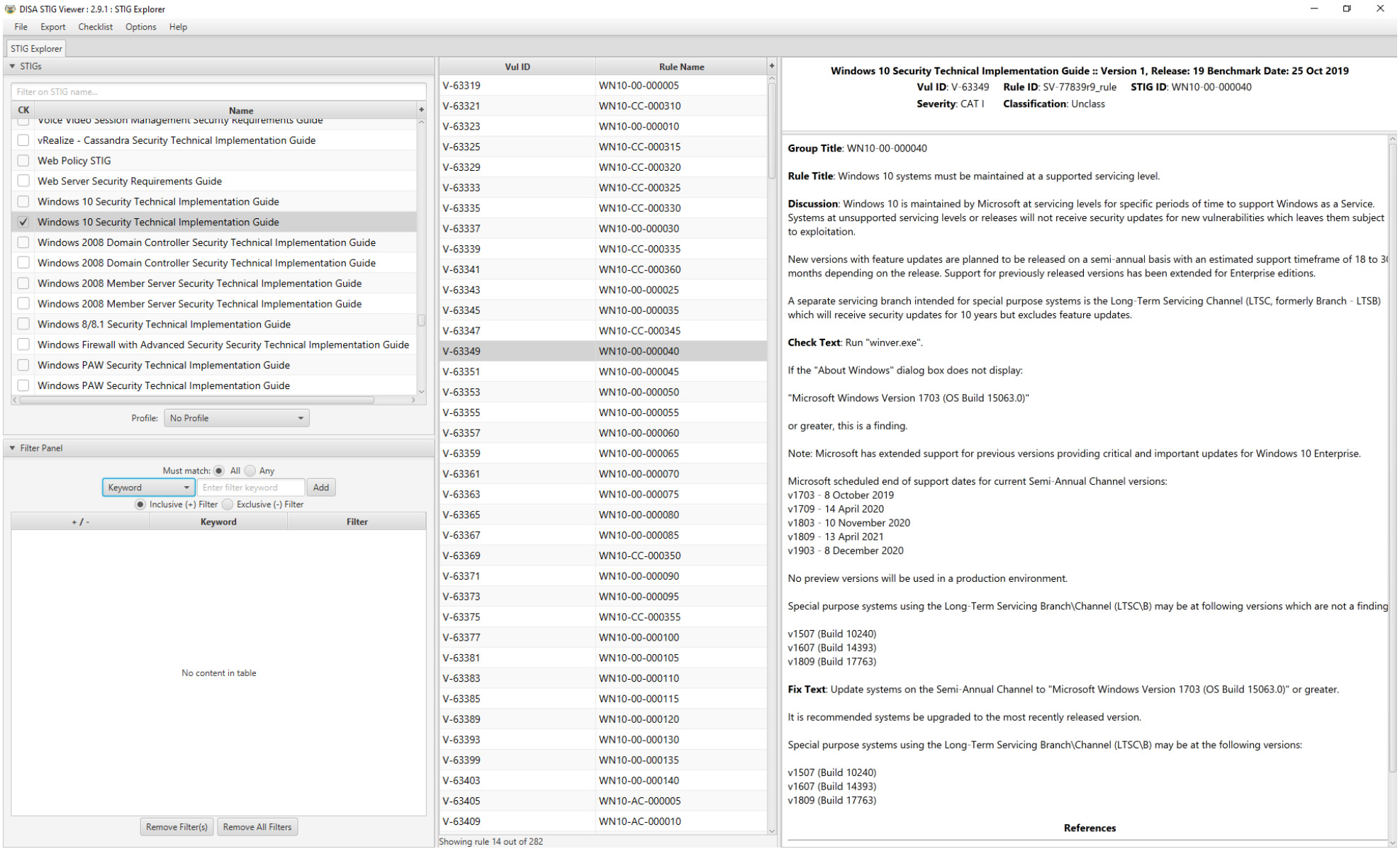
Table of Contents

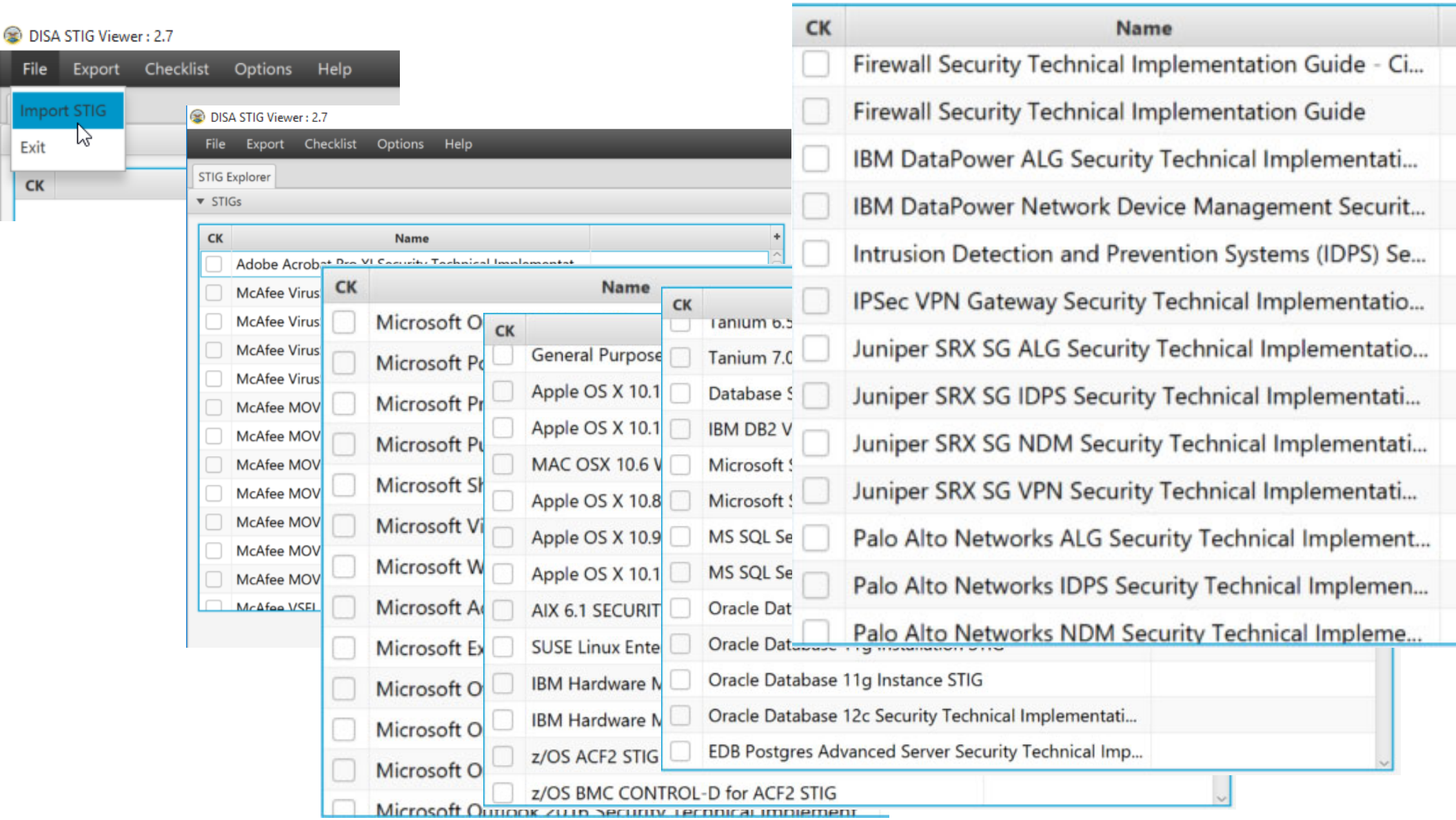
effectiveness

tions/functions

Security Technical Implementation Guides




DISA STIG Viewer : 2.9.1 : STIG Explorer
File
Export
Checklist
Options
Help
STIG Explorer
STIGs
Filter on STIG name...
CK
Name
vRealize - Cassandra Security Technical Implementation Guide
Web Policy STIG
Web Server Security Requirements Guide
Windows 10 Security Technical Implementation Guide
Windows 10 Security Technical Implementation Guide
Windows 2008 Domain Controller Security Technical Implementation Guide
Windows 2008 Domain Controller Security Technical Implementation Guide
Windows 2008 Member Server Security Technical Implementation Guide
Windows 2008 Member Server Security Technical Implementation Guide
Windows 8/8.1 Security Technical Implementation Guide
Windows Firewall with Advanced Security Security Technical Implementation Guide
Windows PAW Security Technical Implementation Guide
Windows PAW Security Technical Implementation Guide
Profile:
No Profile
Filter Panel
Must match:
All
Any
Keyword
Enter filter keyword
Add
Inclusive (+) Filter
Exclusive (-) Filter
+ / -
Keyword
Filter
No content in table
Remove Filter(s)
Remove All Filters
Vul ID
Rule Name
V-63319 WN10-00-000005
V-63321 WN10-CC-000310
V-63323 WN10-00-000010
V-63325 WN10-CC-000315
V-63329 WN10-CC-000320
V-63333 WN10-CC-000325
V-63335 WN10-CC-000330
V-63337 WN10-00-000030
V-63339 WN10-CC-000335
V-63341 WN10-CC-000360
V-63343 WN10-00-000025
V-63345 WN10-00-000035
V-63347 WN10-CC-000345
V-63349 WN10-00-000040
V-63351 WN10-00-000045
V-63353 WN10-00-000050
V-63355 WN10-00-000055
V-63357 WN10-00-000060
V-63359 WN10-00-000065
V-63361 WN10-00-000070
V-63363 WN10-00-000075
V-63365 WN10-00-000080
V-63367 WN10-00-000085
V-63369 WN10-CC-000350
V-63371 WN10-00-000090
V-63373 WN10-00-000095
V-63375 WN10-CC-000355
V-63377 WN10-00-000100
V-63381 WN10-00-000105
V-63383 WN10-00-000110
V-63385 WN10-00-000115
V-63389 WN10-00-000120
V-63393 WN10-00-000130
V-63399 WN10-00-000135
V-63403 WN10-00-000140
V-63405 WN10-AC-000005
V-63409 WN10-AC-000010
Showing rule 14 out of 282
Windows 10 Security Technical Implementation Guide :: Version 1, Release: 19 Benchmark Date: 25 Oct 2019
Vul ID: V-63349 Rule ID: SV-77839r9_rule STIG ID: WN10-00-000040
Severity: CAT I Classification: Unclass
Group Title: WN10-00-000040
Rule Title: Windows 10 systems must be maintained at a supported servicing level.
Discussion: Windows 10 is maintained by Microsoft at servicing levels for specific periods of time to support Windows as a Service. Systems at unsupported servicing levels or releases will not receive security updates for new vulnerabilities which leaves them subject to exploitation.
New versions with feature updates are planned to be released on a semi-annual basis with an estimated support timeframe of 18 to 3
months depending on the release. Support for previously released versions has been extended for Enterprise editions.
A separate servicing branch intended for special purpose systems is the Long-Term Servicing Channel (LTSC, formerly Branch - LTSB) which will receive security updates for 10 years but excludes feature updates.
Check Text: Run "winver.exe".
If the "About Windows" dialog box does not display:
"Microsoft Windows Version 1703 (OS Build 15063.0)"
or greater, this is a finding.
Note: Microsoft has extended support for previous versions providing critical and important updates for Windows 10 Enterprise.
Microsoft scheduled end of support dates for current Semi-Annual Channel versions:
v1703 - 8 October 2019
v1709 - 14 April 2020
v1803 - 10 November 2020
v1809 - 13 April 2021
v1903 - 8 December 2020
No preview versions will be used in a production environment.
Special purpose systems using the Long-Term Servicing Branch\Channel (LTSC\B) may be at following versions which are not a finding
v1507 (Build 10240)
v1607 (Build 14393)
v1809 (Build 17763)
Fix Text: Update systems on the Semi-Annual Channel to "Microsoft Windows Version 1703 (OS Build 15063.0)" or greater.
It is recommended systems be upgraded to the most recently released version.
Special purpose systems using the Long-Term Servicing Branch\Channel (LTSC\B) may be at the following versions:
v1507 (Build 10240)
v1607 (Build 14393)
v1809 (Build 17763)
References


DISA STIG Viewer : 2.7
File
Export
Checklist
Options
Help
Import STIG
Exit
CK
STIG Explorer
STIGs
Name
Adobe Acrobat Pro XI Security Technical Implementat
McAfee Virus
McAfee MOV
Microsoft O
Microsoft P
Microsoft Pr
Microsoft Pu
Microsoft Sh
Microsoft Vi
Microsoft W
Microsoft Ac
Microsoft Ex
Microsoft O
Microsoft Outlook 2010 Security Technical Implement
General Purpose
Apple OS X 10.1
Apple OS X 10.1
MAC OSX 10.6 V
Apple OS X 10.8
Apple OS X 10.9
Apple OS X 10.1
AIX 6.1 SECURIT
SUSE Linux Ente
IBM Hardware M
IBM Hardware M
z/OS ACF2 STIG
z/OS BMC CONTROL-D for ACF2 STIG
Tanium 6.5
Tanium 7.0
Database S
IBM DB2 V
Microsoft S
Microsoft S
MS SQL Se
MS SQL Se
Oracle Dat
Oracle Database 11g Instance STIG
Oracle Database 12c Security Technical Implementati...
EDB Postgres Advanced Server Security Technical Imp...
Firewall Security Technical Implementation Guide - Ci...
Firewall Security Technical Implementation Guide
IBM DataPower ALG Security Technical Implementati...
IBM DataPower Network Device Management Securit...
Intrusion Detection and Prevention Systems (IDPS) Se...
IPSec VPN Gateway Security Technical Implementatio...
Juniper SRX SG ALG Security Technical Implementatio...
Juniper SRX SG IDPS Security Technical Implementati...
Juniper SRX SG NDM Security Technical Implementati...
Juniper SRX SG VPN Security Technical Implementati...
Palo Alto Networks ALG Security Technical Implement...
Palo Alto Networks IDPS Security Technical Implemen...
Palo Alto Networks NDM Security Technical Impleme...

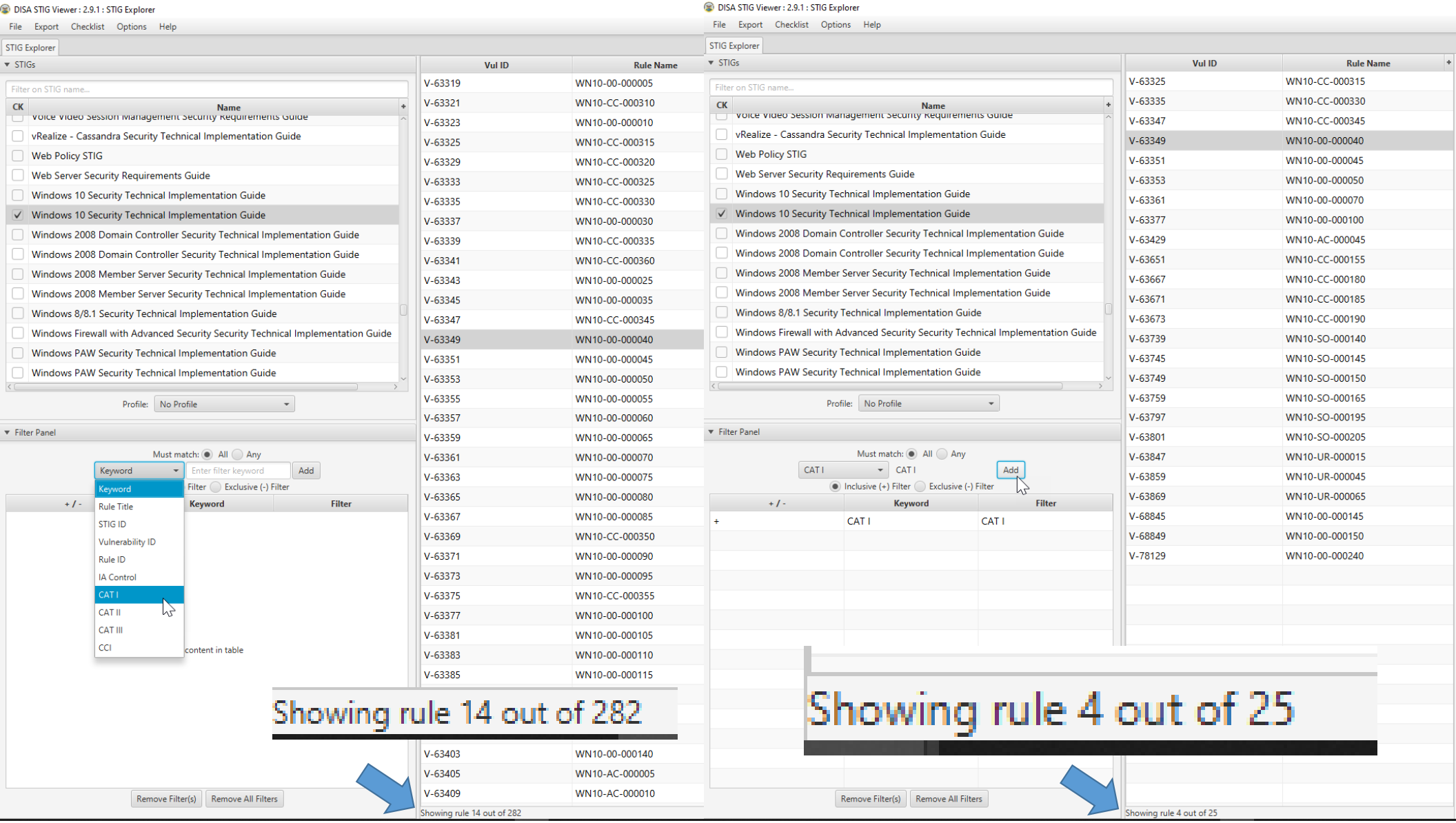
Severity Category Code (CAT) Levels

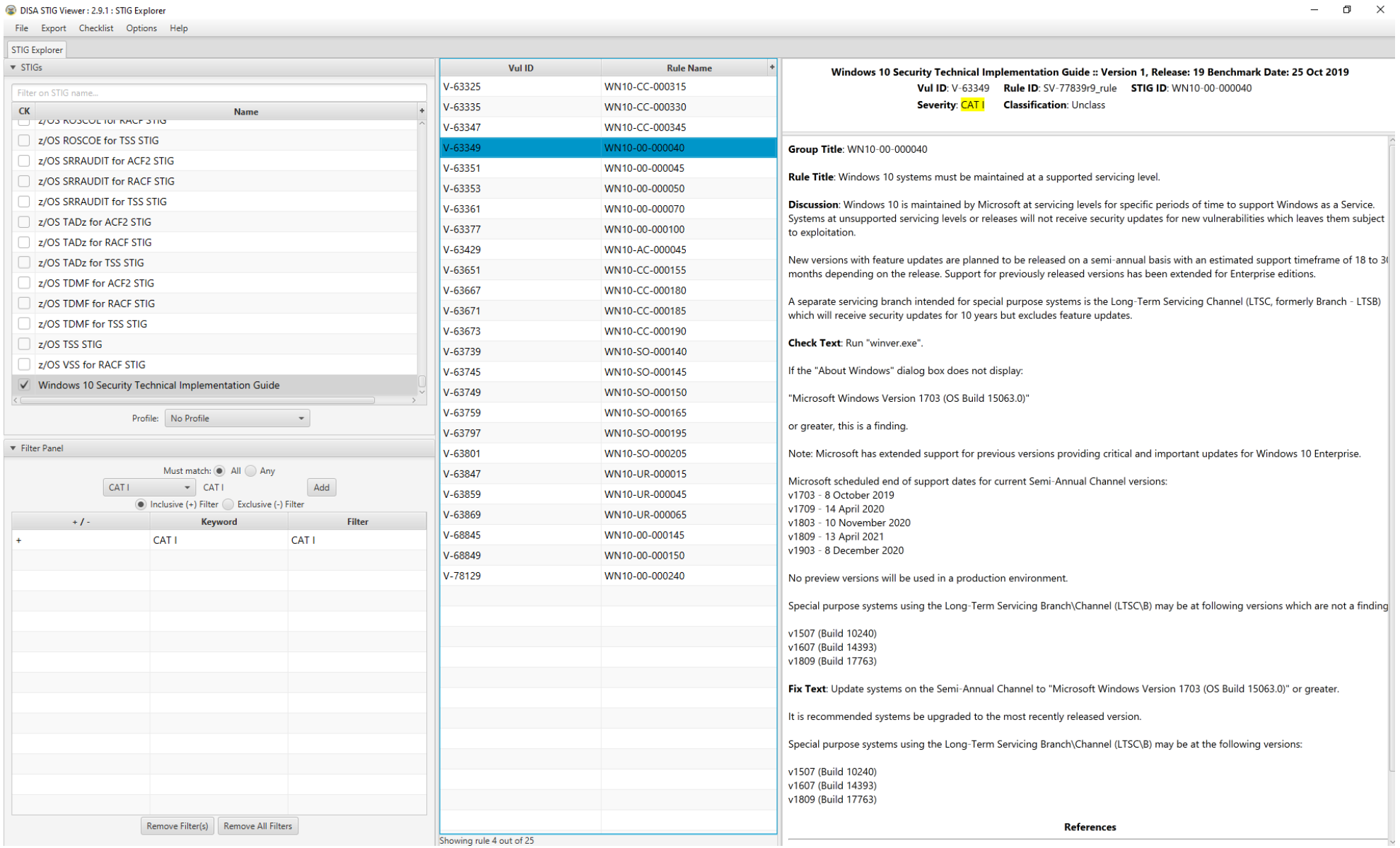
The risk level associated with the information assurance (IA) security weakness and the urgency for a corrective action to be completed

- **CAT I Severity Code** is assigned to *findings* that allow primary security protections to be bypassed, allowing immediate access by unauthorized personnel or unauthorized assumption of super-user privileges
  - CAT I weaknesses **must be corrected** before an Authorization to Operate (ATO) is granted

- **CAT II Severity Code** is assigned to *findings* that have a potential to lead to unauthorized system access or activity.
  - CAT II findings **shall be corrected or satisfactorily mitigated** before an Authorization to Operate will be granted.
  - A system with a CAT II weakness can be granted an ATO only when there is clear evidence that the CAT II weakness can be corrected or satisfactorily mitigated within 180 days of the accreditation decision.

- **CAT III Severity Code** is assigned to r*ecommendations* that will improve IA posture but are **not required** for an authorization to operate


DISA STIG Viewer : 2.9.1 : STIG Explorer
File Export Checklist Options Help
STIG Explorer
STIGs
Filter on STIG name...
CK Name
vRealize - Cassandra Security Technical Implementation Guide
Web Policy STIG
Web Server Security Requirements Guide
Windows 10 Security Technical Implementation Guide
Windows 10 Security Technical Implementation Guide
Windows 2008 Domain Controller Security Technical Implementation Guide
Windows 2008 Domain Controller Security Technical Implementation Guide
Windows 2008 Member Server Security Technical Implementation Guide
Windows 2008 Member Server Security Technical Implementation Guide
Windows 8/8.1 Security Technical Implementation Guide
Windows Firewall with Advanced Security Security Technical Implementation Guide
Windows PAW Security Technical Implementation Guide
Windows PAW Security Technical Implementation Guide
Profile: No Profile
Filter Panel
Must match: All Any
Keyword
Enter filter keyword
Add
Filter Exclusive (-) Filter
+ / - Keyword Filter
Keyword
Rule Title
STIG ID
Vulnerability ID
Rule ID
IA Control
CAT I
CAT II
CAT III
CCI
content in table
Remove Filter(s)
Remove All Filters
Vul ID Rule Name
V-63319 WN10-00-000005
V-63321 WN10-CC-000310
V-63323 WN10-00-000010
V-63325 WN10-CC-000315
V-63329 WN10-CC-000320
V-63333 WN10-CC-000325
V-63335 WN10-CC-000330
V-63337 WN10-00-000030
V-63339 WN10-CC-000335
V-63341 WN10-CC-000360
V-63343 WN10-00-000025
V-63345 WN10-00-000035
V-63347 WN10-CC-000345
V-63349 WN10-00-000040
V-63351 WN10-00-000045
V-63353 WN10-00-000050
V-63355 WN10-00-000055
V-63357 WN10-00-000060
V-63359 WN10-00-000065
V-63361 WN10-00-000070
V-63363 WN10-00-000075
V-63365 WN10-00-000080
V-63367 WN10-00-000085
V-63369 WN10-CC-000350
V-63371 WN10-00-000090
V-63373 WN10-00-000095
V-63375 WN10-CC-000355
V-63377 WN10-00-000100
V-63381 WN10-00-000105
V-63383 WN10-00-000110
V-63385 WN10-00-000115
V-63403 WN10-00-000140
V-63405 WN10-AC-000005
V-63409 WN10-AC-000010
Showing rule 14 out of 282
Showing rule 14 out of 282
DISA STIG Viewer : 2.9.1 : STIG Explorer
File Export Checklist Options Help
STIG Explorer
STIGs
Filter on STIG name...
CK Name
vRealize - Cassandra Security Technical Implementation Guide
Web Policy STIG
Web Server Security Requirements Guide
Windows 10 Security Technical Implementation Guide
Windows 10 Security Technical Implementation Guide
Windows 2008 Domain Controller Security Technical Implementation Guide
Windows 2008 Domain Controller Security Technical Implementation Guide
Windows 2008 Member Server Security Technical Implementation Guide
Windows 2008 Member Server Security Technical Implementation Guide
Windows 8/8.1 Security Technical Implementation Guide
Windows Firewall with Advanced Security Security Technical Implementation Guide
Windows PAW Security Technical Implementation Guide
Windows PAW Security Technical Implementation Guide
Profile: No Profile
Filter Panel
Must match: All Any
CAT I
CAT I
Add
Inclusive (+) Filter Exclusive (-) Filter
+ / - Keyword Filter
+ CAT I CAT I
Remove Filter(s)
Remove All Filters
Vul ID Rule Name
V-63325 WN10-CC-000315
V-63335 WN10-CC-000330
V-63347 WN10-CC-000345
V-63349 WN10-00-000040
V-63351 WN10-00-000045
V-63353 WN10-00-000050
V-63361 WN10-00-000070
V-63377 WN10-00-000100
V-63429 WN10-AC-000045
V-63651 WN10-CC-000155
V-63667 WN10-CC-000180
V-63671 WN10-CC-000185
V-63673 WN10-CC-000190
V-63739 WN10-SO-000140
V-63745 WN10-SO-000145
V-63749 WN10-SO-000150
V-63759 WN10-SO-000165
V-63797 WN10-SO-000195
V-63801 WN10-SO-000205
V-63847 WN10-UR-000015
V-63859 WN10-UR-000045
V-63869 WN10-UR-000065
V-68845 WN10-00-000145
V-68849 WN10-00-000150
V-78129 WN10-00-000240
Showing rule 4 out of 25
Showing rule 4 out of 25


DISA STIG Viewer : 2.9.1 : STIG Explorer
File
Export
Checklist
Options
Help
STIG Explorer
STIGs
Filter on STIG name...
CK
Name
z/OS ROSCOE for TSS STIG
z/OS SRRAUDIT for ACF2 STIG
z/OS SRRAUDIT for RACF STIG
z/OS SRRAUDIT for TSS STIG
z/OS TADz for ACF2 STIG
z/OS TADz for RACF STIG
z/OS TADz for TSS STIG
z/OS TDMF for ACF2 STIG
z/OS TDMF for RACF STIG
z/OS TDMF for TSS STIG
z/OS TSS STIG
z/OS VSS for RACF STIG
Windows 10 Security Technical Implementation Guide
Profile:
No Profile
Filter Panel
Must match:
All
Any
CAT I
CAT I
Add
Inclusive (+) Filter
Exclusive (-) Filter
+ / -
Keyword
Filter
+
CAT I
CAT I
Remove Filter(s)
Remove All Filters
Vul ID
Rule Name
V-63325
WN10-CC-000315
V-63335
WN10-CC-000330
V-63347
WN10-CC-000345
V-63349
WN10-00-000040
V-63351
WN10-00-000045
V-63353
WN10-00-000050
V-63361
WN10-00-000070
V-63377
WN10-00-000100
V-63429
WN10-AC-000045
V-63651
WN10-CC-000155
V-63667
WN10-CC-000180
V-63671
WN10-CC-000185
V-63673
WN10-CC-000190
V-63739
WN10-SO-000140
V-63745
WN10-SO-000145
V-63749
WN10-SO-000150
V-63759
WN10-SO-000165
V-63797
WN10-SO-000195
V-63801
WN10-SO-000205
V-63847
WN10-UR-000015
V-63859
WN10-UR-000045
V-63869
WN10-UR-000065
V-68845
WN10-00-000145
V-68849
WN10-00-000150
V-78129
WN10-00-000240
Showing rule 4 out of 25
Windows 10 Security Technical Implementation Guide :: Version 1, Release: 19 Benchmark Date: 25 Oct 2019
Vul ID: V-63349
Rule ID: SV-77839r9_rule
STIG ID: WN10-00-000040
Severity: CAT I
Classification: Unclass
Group Title: WN10-00-000040
Rule Title: Windows 10 systems must be maintained at a supported servicing level.
Discussion: Windows 10 is maintained by Microsoft at servicing levels for specific periods of time to support Windows as a Service. Systems at unsupported servicing levels or releases will not receive security updates for new vulnerabilities which leaves them subject to exploitation.
New versions with feature updates are planned to be released on a semi-annual basis with an estimated support timeframe of 18 to 3
months depending on the release. Support for previously released versions has been extended for Enterprise editions.
A separate servicing branch intended for special purpose systems is the Long-Term Servicing Channel (LTSC, formerly Branch - LTSB) which will receive security updates for 10 years but excludes feature updates.
Check Text: Run "winver.exe".
If the "About Windows" dialog box does not display:
"Microsoft Windows Version 1703 (OS Build 15063.0)"
or greater, this is a finding.
Note: Microsoft has extended support for previous versions providing critical and important updates for Windows 10 Enterprise.
Microsoft scheduled end of support dates for current Semi-Annual Channel versions:
v1703 - 8 October 2019
v1709 - 14 April 2020
v1803 - 10 November 2020
v1809 - 13 April 2021
v1903 - 8 December 2020
No preview versions will be used in a production environment.
Special purpose systems using the Long-Term Servicing Branch\Channel (LTSC\B) may be at following versions which are not a finding
v1507 (Build 10240)
v1607 (Build 14393)
v1809 (Build 17763)
Fix Text: Update systems on the Semi-Annual Channel to "Microsoft Windows Version 1703 (OS Build 15063.0)" or greater.
It is recommended systems be upgraded to the most recently released version.
Special purpose systems using the Long-Term Servicing Branch\Channel (LTSC\B) may be at the following versions:
v1507 (Build 10240)
v1607 (Build 14393)
v1809 (Build 17763)
References

Check Text: Run "winver.exe".

If the "About Windows" dialog box does not display:

"Microsoft Windows Version 1703 (OS Build 15063.0)"

or greater, this is a finding.

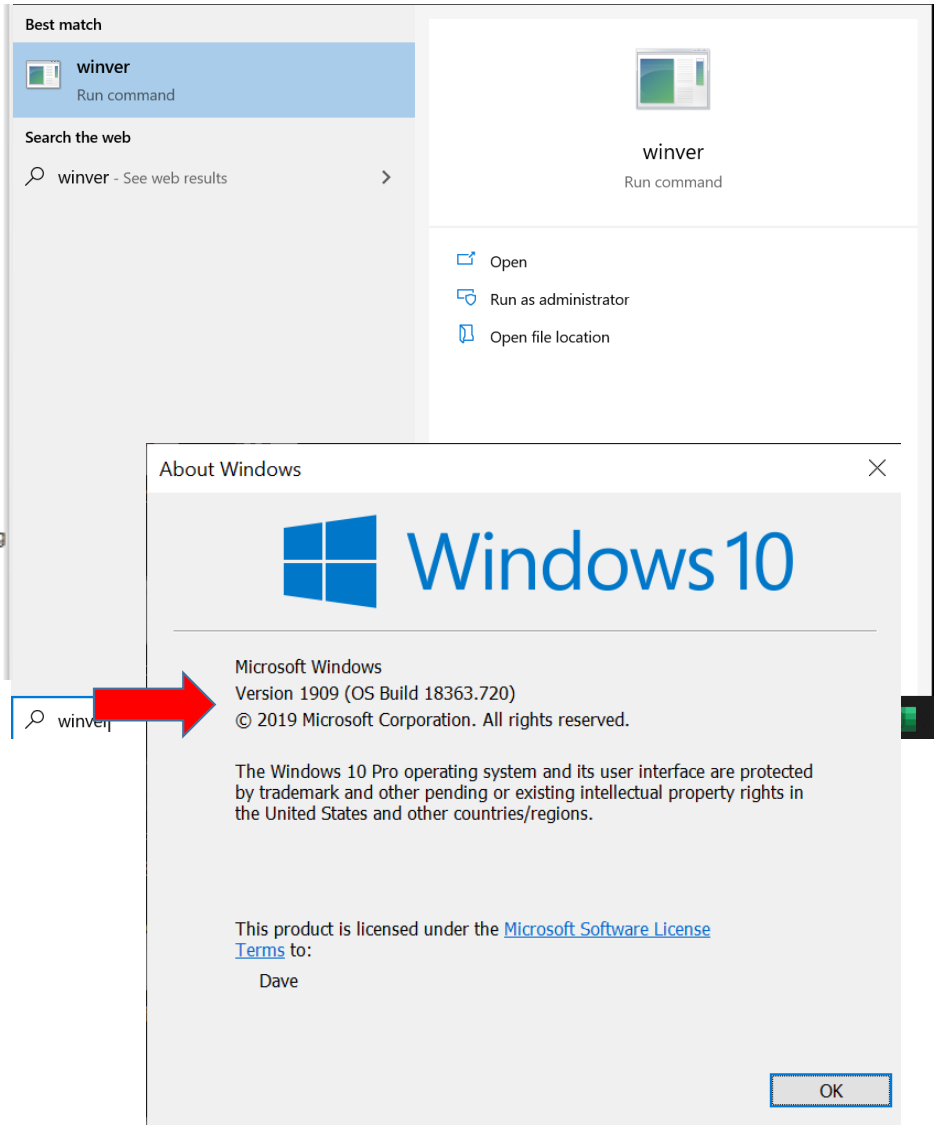
Note: Microsoft has extended support for previous versions providing critical and important updates for Windows 10 Enterprise.

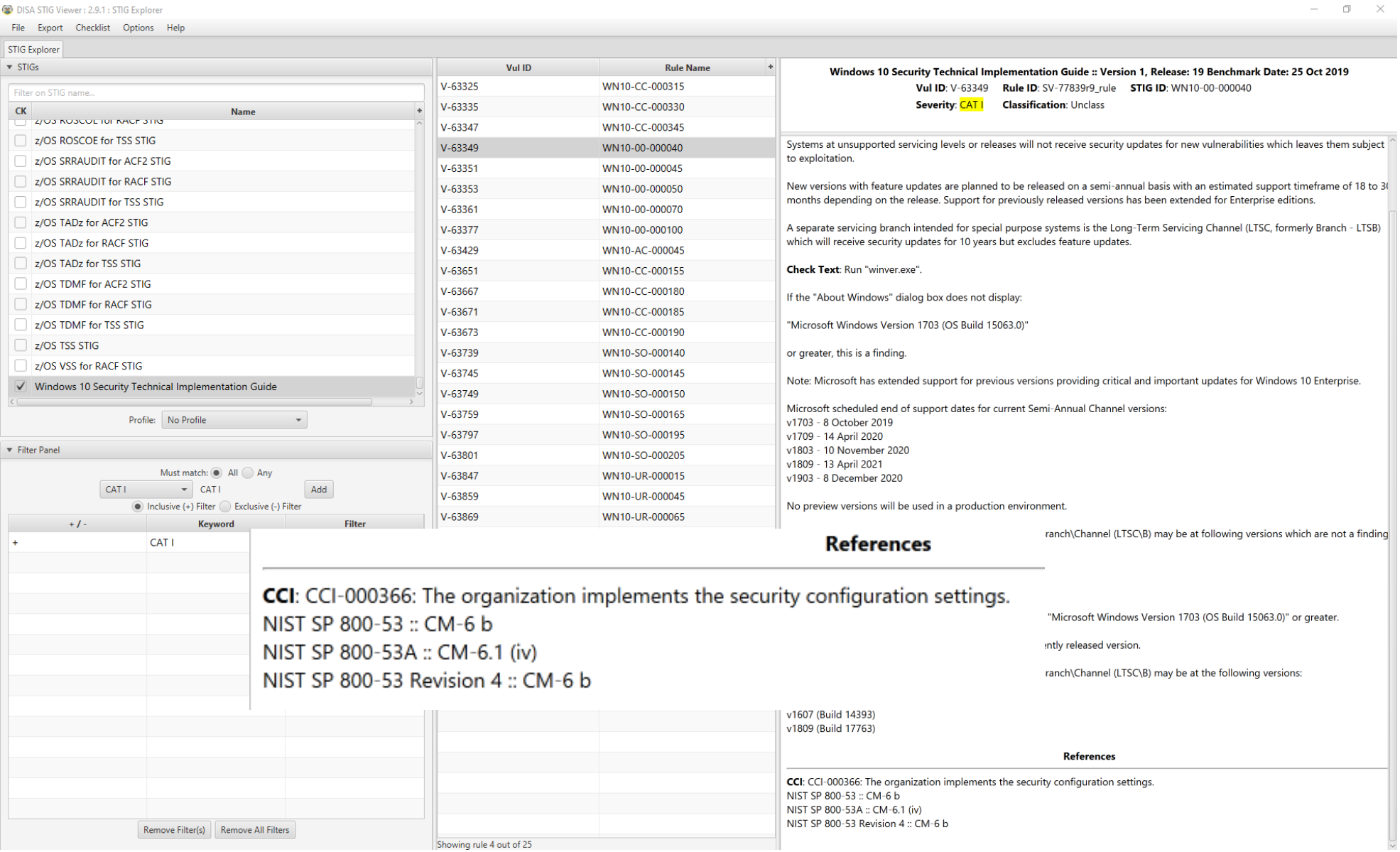
Microsoft scheduled end of support dates for current Semi-Annual Channel versions:
v1703 - 8 October 2019
v1709 - 14 April 2020
v1803 - 10 November 2020
v1809 - 13 April 2021
v1903 - 8 December 2020

No preview versions will be used in a production environment.

Special purpose systems using the Long-Term Servicing Branch\Channel (LTSC\B) may be at following versions which are not a finding

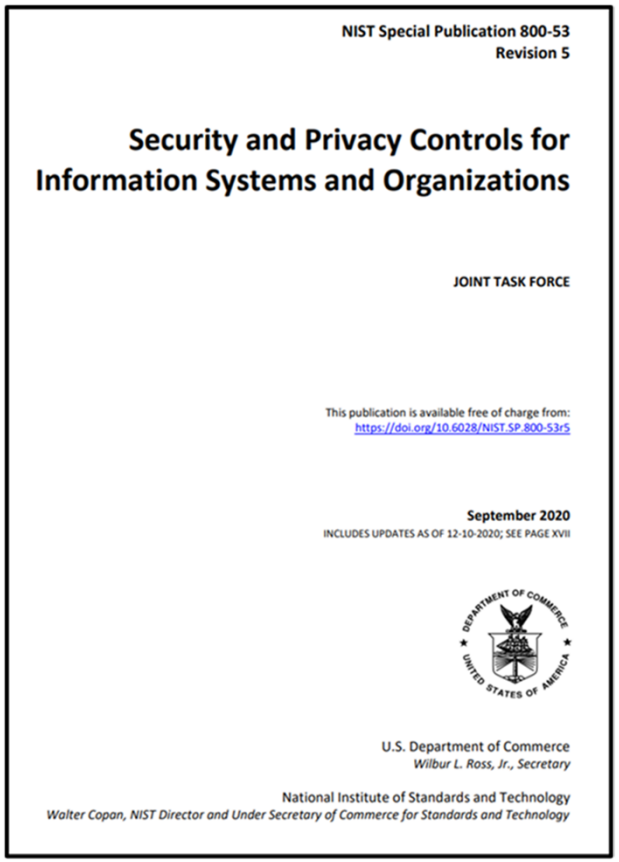
v1507 (Build 10240)
v1607 (Build 14393)
v1809 (Build 17763)




DISA STIG Viewer : 2.9.1 : STIG Explorer
File Export Checklist Options Help
STIG Explorer
STIGs
Filter on STIG name...
CK Name
z/OS ROSCOE for TSS STIG
z/OS SRRAUDIT for ACF2 STIG
z/OS SRRAUDIT for RACF STIG
z/OS SRRAUDIT for TSS STIG
z/OS TADz for ACF2 STIG
z/OS TADz for RACF STIG
z/OS TADz for TSS STIG
z/OS TDMF for ACF2 STIG
z/OS TDMF for RACF STIG
z/OS TDMF for TSS STIG
z/OS TSS STIG
z/OS VSS for RACF STIG
Windows 10 Security Technical Implementation Guide
Profile: No Profile
Filter Panel
Must match: All Any
CAT I CAT I Add
Inclusive (+) Filter Exclusive (-) Filter
+ / - Keyword Filter
+ CAT I
Remove Filter(s) Remove All Filters
Vul ID Rule Name
V-63325 WN10-CC-000315
V-63335 WN10-CC-000330
V-63347 WN10-CC-000345
V-63349 WN10-00-000040
V-63351 WN10-00-000045
V-63353 WN10-00-000050
V-63361 WN10-00-000070
V-63377 WN10-00-000100
V-63429 WN10-AC-000045
V-63651 WN10-CC-000155
V-63667 WN10-CC-000180
V-63671 WN10-CC-000185
V-63673 WN10-CC-000190
V-63739 WN10-SO-000140
V-63745 WN10-SO-000145
V-63749 WN10-SO-000150
V-63759 WN10-SO-000165
V-63797 WN10-SO-000195
V-63801 WN10-SO-000205
V-63847 WN10-UR-000015
V-63859 WN10-UR-000045
V-63869 WN10-UR-000065
Showing rule 4 out of 25
Windows 10 Security Technical Implementation Guide :: Version 1, Release: 19 Benchmark Date: 25 Oct 2019
Vul ID: V-63349 Rule ID: SV-77839r9_rule STIG ID: WN10-00-000040
Severity: CAT I Classification: Unclass
Systems at unsupported servicing levels or releases will not receive security updates for new vulnerabilities which leaves them subject to exploitation.
New versions with feature updates are planned to be released on a semi-annual basis with an estimated support timeframe of 18 to 3
months depending on the release. Support for previously released versions has been extended for Enterprise editions.
A separate servicing branch intended for special purpose systems is the Long-Term Servicing Channel (LTSC, formerly Branch - LTSB) which will receive security updates for 10 years but excludes feature updates.
Check Text: Run "winver.exe".
If the "About Windows" dialog box does not display:
"Microsoft Windows Version 1703 (OS Build 15063.0)"
or greater, this is a finding.
Note: Microsoft has extended support for previous versions providing critical and important updates for Windows 10 Enterprise.
Microsoft scheduled end of support dates for current Semi-Annual Channel versions:
v1703 - 8 October 2019
v1709 - 14 April 2020
v1803 - 10 November 2020
v1809 - 13 April 2021
v1903 - 8 December 2020
No preview versions will be used in a production environment.
References
CCI: CCI-000366: The organization implements the security configuration settings.
NIST SP 800-53 :: CM-6 b
NIST SP 800-53A :: CM-6.1 (iv)
NIST SP 800-53 Revision 4 :: CM-6 b
ranch\Channel (LTSC\B) may be at following versions which are not a finding
"Microsoft Windows Version 1703 (OS Build 15063.0)" or greater.
ntly released version.
ranch\Channel (LTSC\B) may be at the following versions:
v1607 (Build 14393)
v1809 (Build 17763)
References
CCI: CCI-000366: The organization implements the security configuration settings.
NIST SP 800-53 :: CM-6 b
NIST SP 800-53A :: CM-6.1 (iv)
NIST SP 800-53 Revision 4 :: CM-6 b

References

CCI: CCI-000366: The organization implements the security configuration settings.
NIST SP 800-53 :: CM-6 b
NIST SP 800-53A :: CM-6.1 (iv)
NIST SP 800-53 Revision 4 :: CM-6 b



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

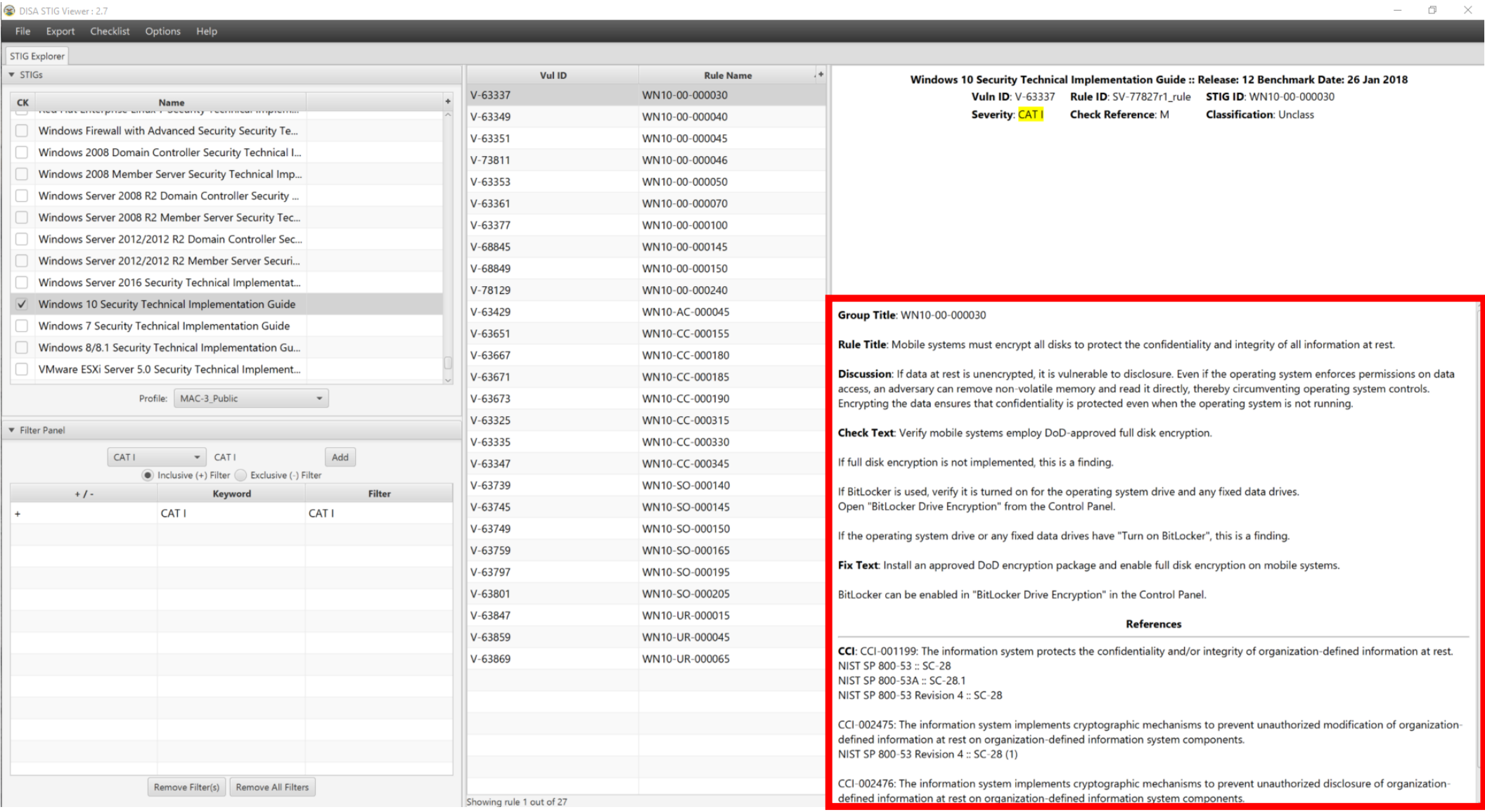
This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

CM-6(1)	CONFIGURATION SETTINGS | *AUTOMATED CENTRAL MANAGEMENT / APPLICATION / VERIFICATION*	
	ASSESSMENT OBJECTIVE: *Determine if the organization:*	
	CM-6(1)[1]	*defines information system components for which automated mechanisms are to be employed to:*
		CM-6(1)[1][a] *centrally manage configuration settings of such components;*
		CM-6(1)[1][b] *apply configuration settings of such components;*
		CM-6(1)[1][c] *verify configuration settings of such components;*
	CM-6(1)[2]	*employs automated mechanisms to:*
		CM-6(1)[2][a] *centrally manage configuration settings for organization-defined information system components;*
		CM-6(1)[2][b] *apply configuration settings for organization-defined information system components; and*
		CM-6(1)[2][c] *verify configuration settings for organization-defined information system components.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Configuration management policy; procedures addressing configuration settings for the information system; configuration management plan; information system design documentation; information system configuration settings and associated documentation; security configuration checklists; change control records; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with security configuration management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers]. **Test**: [*SELECT FROM:* Organizational processes for managing configuration settings; automated mechanisms implemented to centrally manage, apply, and verify information system configuration settings].	


DISA STIG Viewer : 2.7
File
Export
Checklist
Options
Help
STIG Explorer
STIGs
CK
Name
Windows Firewall with Advanced Security Security Te...
Windows 2008 Domain Controller Security Technical I...
Windows 2008 Member Server Security Technical Imp...
Windows Server 2008 R2 Domain Controller Security ...
Windows Server 2008 R2 Member Server Security Tec...
Windows Server 2012/2012 R2 Domain Controller Sec...
Windows Server 2012/2012 R2 Member Server Securi...
Windows Server 2016 Security Technical Implementat...
Windows 10 Security Technical Implementation Guide
Windows 7 Security Technical Implementation Guide
Windows 8/8.1 Security Technical Implementation Gu...
VMware ESXi Server 5.0 Security Technical Implement...
Profile:
MAC-3_Public
Filter Panel
CAT I
CAT I
Add
Inclusive (+) Filter
Exclusive (-) Filter
+ / -
Keyword
Filter
+
CAT I
CAT I
Remove Filter(s)
Remove All Filters
Vul ID
Rule Name
V-63337
WN10-00-000030
V-63349
WN10-00-000040
V-63351
WN10-00-000045
V-73811
WN10-00-000046
V-63353
WN10-00-000050
V-63361
WN10-00-000070
V-63377
WN10-00-000100
V-68845
WN10-00-000145
V-68849
WN10-00-000150
V-78129
WN10-00-000240
V-63429
WN10-AC-000045
V-63651
WN10-CC-000155
V-63667
WN10-CC-000180
V-63671
WN10-CC-000185
V-63673
WN10-CC-000190
V-63325
WN10-CC-000315
V-63335
WN10-CC-000330
V-63347
WN10-CC-000345
V-63739
WN10-SO-000140
V-63745
WN10-SO-000145
V-63749
WN10-SO-000150
V-63759
WN10-SO-000165
V-63797
WN10-SO-000195
V-63801
WN10-SO-000205
V-63847
WN10-UR-000015
V-63859
WN10-UR-000045
V-63869
WN10-UR-000065
Showing rule 1 out of 27
Windows 10 Security Technical Implementation Guide :: Release: 12 Benchmark Date: 26 Jan 2018
Vuln ID: V-63337
Rule ID: SV-77827r1_rule
STIG ID: WN10-00-000030
Severity: CAT I
Check Reference: M
Classification: Unclass
Group Title: WN10-00-000030
Rule Title: Mobile systems must encrypt all disks to protect the confidentiality and integrity of all information at rest.
Discussion: If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running.
Check Text: Verify mobile systems employ DoD-approved full disk encryption.
If full disk encryption is not implemented, this is a finding.
If BitLocker is used, verify it is turned on for the operating system drive and any fixed data drives.
Open "BitLocker Drive Encryption" from the Control Panel.
If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding.
Fix Text: Install an approved DoD encryption package and enable full disk encryption on mobile systems.
BitLocker can be enabled in "BitLocker Drive Encryption" in the Control Panel.
References
CCI: CCI-001199: The information system protects the confidentiality and/or integrity of organization-defined information at rest.
NIST SP 800-53 :: SC-28
NIST SP 800-53A :: SC-28.1
NIST SP 800-53 Revision 4 :: SC-28
CCI-002475: The information system implements cryptographic mechanisms to prevent unauthorized modification of organization-defined information at rest on organization-defined information system components.
NIST SP 800-53 Revision 4 :: SC-28 (1)
CCI-002476: The information system implements cryptographic mechanisms to prevent unauthorized disclosure of organization-defined information at rest on organization-defined information system components.

Group Title: WN10-00-000030

Rule Title: Mobile systems must encrypt all disks to protect the confidentiality and integrity of all information at rest.

Discussion: If data at rest is unencrypted, it is vulnerable to disclosure. Even if the operating system enforces permissions on data access, an adversary can remove non-volatile memory and read it directly, thereby circumventing operating system controls. Encrypting the data ensures that confidentiality is protected even when the operating system is not running.

Check Text: Verify mobile systems employ DoD-approved full disk encryption.

If full disk encryption is not implemented, this is a finding.

If BitLocker is used, verify it is turned on for the operating system drive and any fixed data drives.
Open "BitLocker Drive Encryption" from the Control Panel.

If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding.

Fix Text: Install an approved DoD encryption package and enable full disk encryption on mobile systems.

BitLocker can be enabled in "BitLocker Drive Encryption" in the Control Panel.

Check Text: Verify mobile systems employ DoD-approved full disk encryption.

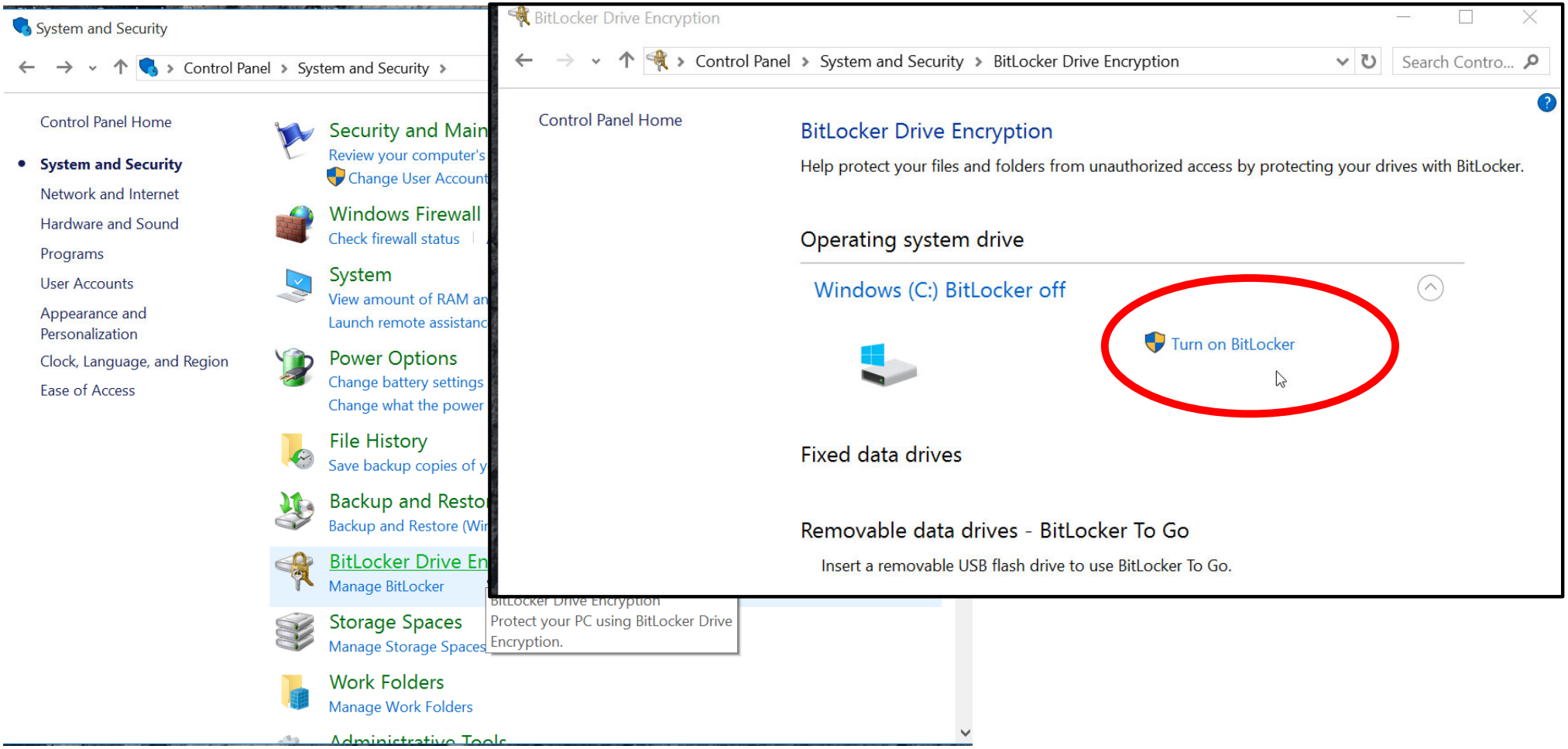
If full disk encryption is not implemented, this is a finding.

If BitLocker is used, verify it is turned on for the operating system drive and any fixed data drives.
Open "BitLocker Drive Encryption" from the Control Panel.

If the operating system drive or any fixed data drives have "Turn on BitLocker", this is a finding.

Fix Text: Install an approved DoD encryption package and enable full disk encryption on mobile systems.

BitLocker can be enabled in "BitLocker Drive Encryption" in the Control Panel.


System and Security
Control Panel › System and Security ›
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock, Language, and Region
Ease of Access
Security and Main
Review your computer's
Change User Account
Windows Firewall
Check firewall status
System
View amount of RAM an
Launch remote assistanc
Power Options
Change battery settings
Change what the power
File History
Save backup copies of y
Backup and Resto
Backup and Restore (Wi
BitLocker Drive En
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Administrative Tools
Protect your PC using BitLocker Drive Encryption.
BitLocker Drive Encryption
Control Panel › System and Security › BitLocker Drive Encryption
Search Contro...
Control Panel Home
BitLocker Drive Encryption
Help protect your files and folders from unauthorized access by protecting your drives with BitLocker.
Operating system drive
Windows (C:) BitLocker off
Turn on BitLocker
Fixed data drives
Removable data drives - BitLocker To Go
Insert a removable USB flash drive to use BitLocker To Go.

Agenda

- ✓Risk Management Framework – A quick review…
- ✓Implementing controls – Host hardening…
  - ✓Security configuration checklist (w/DISA STIG Viewer)
- SCAP - Security Content Automation Protocol
- System Security Plan's Section 13
  - Select 1 control family to fill out for your information system
- Team Project - SSP draft development…

SCAP (Security Content Automation Protocol) *pronounced "ess-cap"*

Purpose: Used for continuously monitoring deployed computer systems and applications for detectable vulnerabilities and assure they incorporate security upgrades to software ("patches") and deploy updates to configurations

SCAP based on a number of open standards, widely used to enumerate software flaws and configuration issues related to security

- The National Vulnerability Database (NVD) is the U.S. government content repository for SCAP
  - *Vendors can get their computer system configuration scanner product validated against SCAP, demonstrating that it will interoperate with other scanners and express the scan results in a standardized way*
- Validated tools for automating collection of assessment objects used in Examine, Inspect and Test activities

https://en.wikipedia.org/wiki/Security_Content_Automation_Protocol

Examine: SCAP (Security Content Automation Protocol) validated tools may be used to automate collection of assessment objects

Common SCAP uses

- Security configuration verification
  - Compare settings in a checklist to a system's actual configuration
  - Verify configuration before deployment, audit/assess/monitor operational systems
  - Map individual settings to high-level requirements (requirements traceability)
  - Verifying patch installation and identifying missing patches

- Check systems for signs of compromise
  - Known characteristics of attacks, such as altered files or the presence of a malicious service

Frequently Asked Questions – FAQs
Group Policy Objects
Quarterly Release Schedule and Summary
SRG / STIG Library Compilations
SRG / STIG Mailing List
SRG/STIG Tools and Viewing Guidance
Sunset Products
Vendor STIG Development Process
Help

SCAP 1.2 CONTENT

Show 10 entries Search:

TITLE	SIZE	UPDATED
Adobe Acrobat Reader DC Classic Track STIG Benchmark - Ver 2, Rel 1	10.95 KB	26 Oct 2020
Adobe Acrobat Reader DC Continuous Track STIG Benchmark - Ver 2, Rel 1	10.79 KB	26 Jul 2021
Canonical Ubuntu 18.04 STIG Benchmark - Ver 2, Rel 5	50.75 KB	24 Jan 2022
Canonical Ubuntu 20.04 LTS STIG Benchmark - Ver 1, Rel 1	59.4 KB	24 Feb 2022
Google Chrome Current Windows STIG Benchmark - Ver 2, Rel 5	24.1 KB	24 Jan 2022
Microsoft .Net Framework 4 STIG Benchmark - Ver 2, Rel 1	8.44 KB	22 Jan 2021
Microsoft Edge STIG Benchmark - Ver 1, Rel 1	24.23 KB	27 Oct 2021
Microsoft Windows 10 STIG Benchmark - Ver 2, Rel 3	100.5 KB	18 Nov 2021
Microsoft Windows Defender Antivirus STIG Benchmark - Ver 2, Rel 2	22.31 KB	18 Nov 2021
Microsoft Windows Firewall STIG Benchmark - Ver 2, Rel 1	13.53 KB	18 Nov 2021

Showing 1 to 10 of 26 entries Previous 1 2 3 Next

SCAP TOOLS

Show 10 entries Search:

TITLE	SIZE	UPDATED
SCC 5.4.2 Checksum file	7.56 KB	15 Sep 2021

SecurityCenter | Dashboard | Analysis | Scans | Reporting | Assets | Workflow | Hi, cody [cody]

SCAP Audit Summary

Switch Dashboard

SCAP Audit Summary - Top 25 Linux Compliance Failed Checks

Plugin ID	Name	Severity	Total
1003887	CCE-18031-5::ipsec_tools_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configurati...	High	1
10038...	CCE-17504-2::irda_tools_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configurati...	High	1
10038...	CCE-18200-6::talk_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configuration_ba...	High	1
10038...	CCE-17250-2::pam_ccreds_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configura...	High	1
10038...	CCE-17742-8::usgcb-rhel5desktop-rule-2.6.1.0:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_...	High	1
1003881	CCE-15018-5::postfix_network_listening:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_config...	High	1
10038...	CCE-14068-1::postfix_package_installation:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_co...	High	1
10038...	CCE-14495-6::sendmail_package_installation:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_...	High	1
1003878	CCE-14825-4::isdn4k_utils_package:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configura...	High	1
10038...	CCE-14412-1::nodev_option_on_tmp:USGCB-RHEL-5-Desktop_1.2.5.0:united_states_government_configura...	High	1

Last Updated: 1 hour ago

SCAP Audit Summary - Top 25 Windows Compliance Failed Checks

Plugin ID	Name	Severit...	T...
10046...	CCE-14830-4::SV-25139r1_rule:Windows_7_STIG_1:MAC-1_Public	High	1
10046...	CCE-14109-3::SV-25138r1_rule:Windows_7_STIG_1:MAC-1_Public	High	1
10046...	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) must be installed on the system.VMS Target Wi...	High	1
10046...	CCE-15041-7::SV-25143r1_rule:Windows_7_STIG_1:MAC-1_Public	High	1
10046...	CCE-10777-1::SV-25107r1_rule:Windows_7_STIG_1:MAC-1_Public	High	1
10046...	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) system-wide Address Space Layout Randomizat...	High	1
10046...	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) system-wide Data Execution Prevention (DEP) ...	High	1
1004641	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Popular Software is not e...	High	1
10046...	noCCE:The Enhanced Mitigation Experience Toolkit (EMET) Default Protections for Internet Explorer must b...	High	1
10046...	noCCE:Local administrator accounts must have their privileged token filtered to prevent elevated privileges ...	High	1

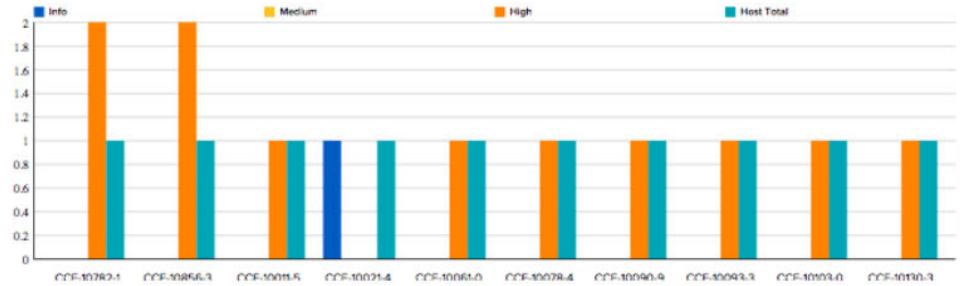
Last Updated: 1 hour ago

SCAP Audit Summary - Compliance Summary

	Systems	Passed	Manual Check	Failed
Windows	1	30%	3%	67%
Linux	1	39%	13%	47%

Last Updated: 1 hour ago

SCAP Audit Summary - Top 10 CCE's

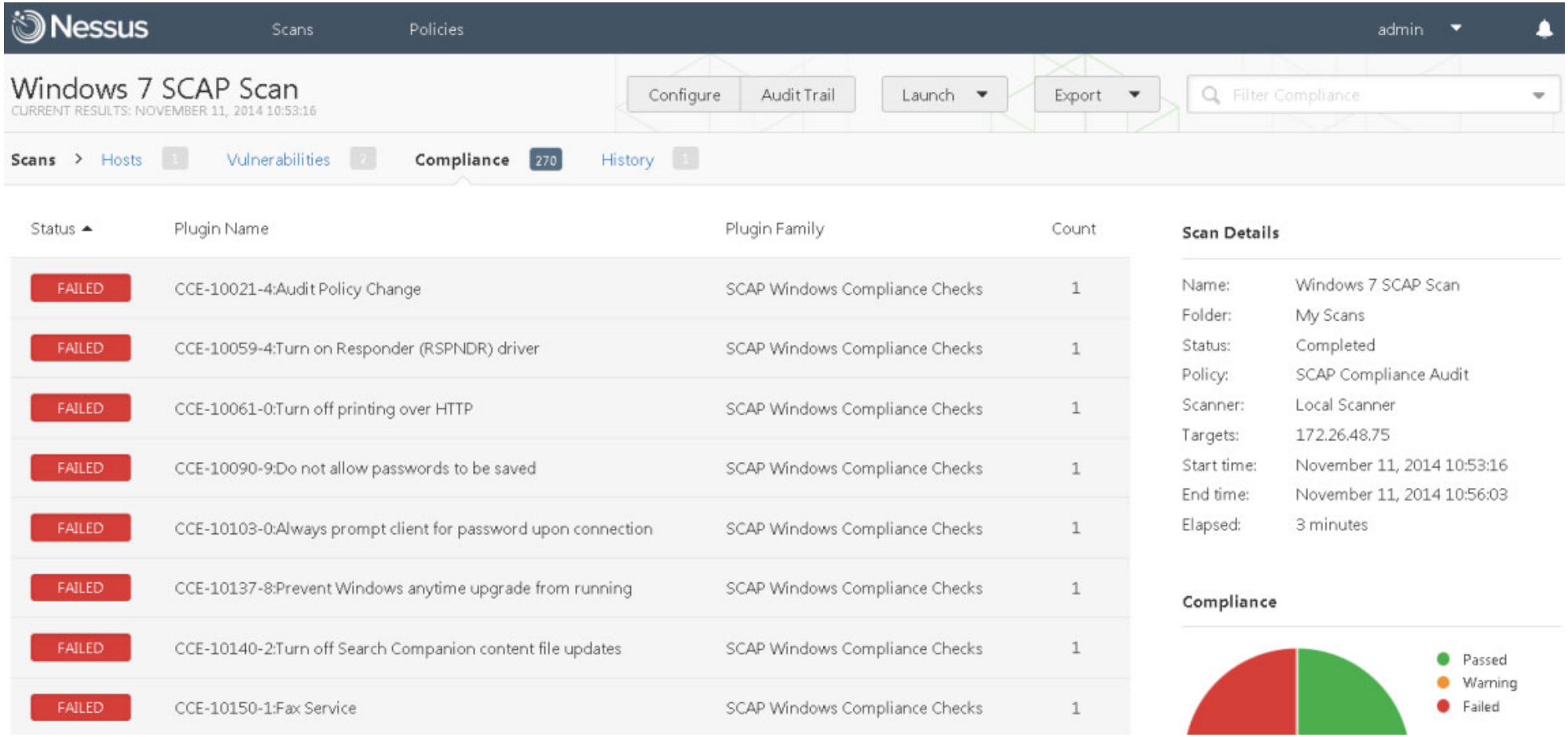


Last Updated: 1 hour ago

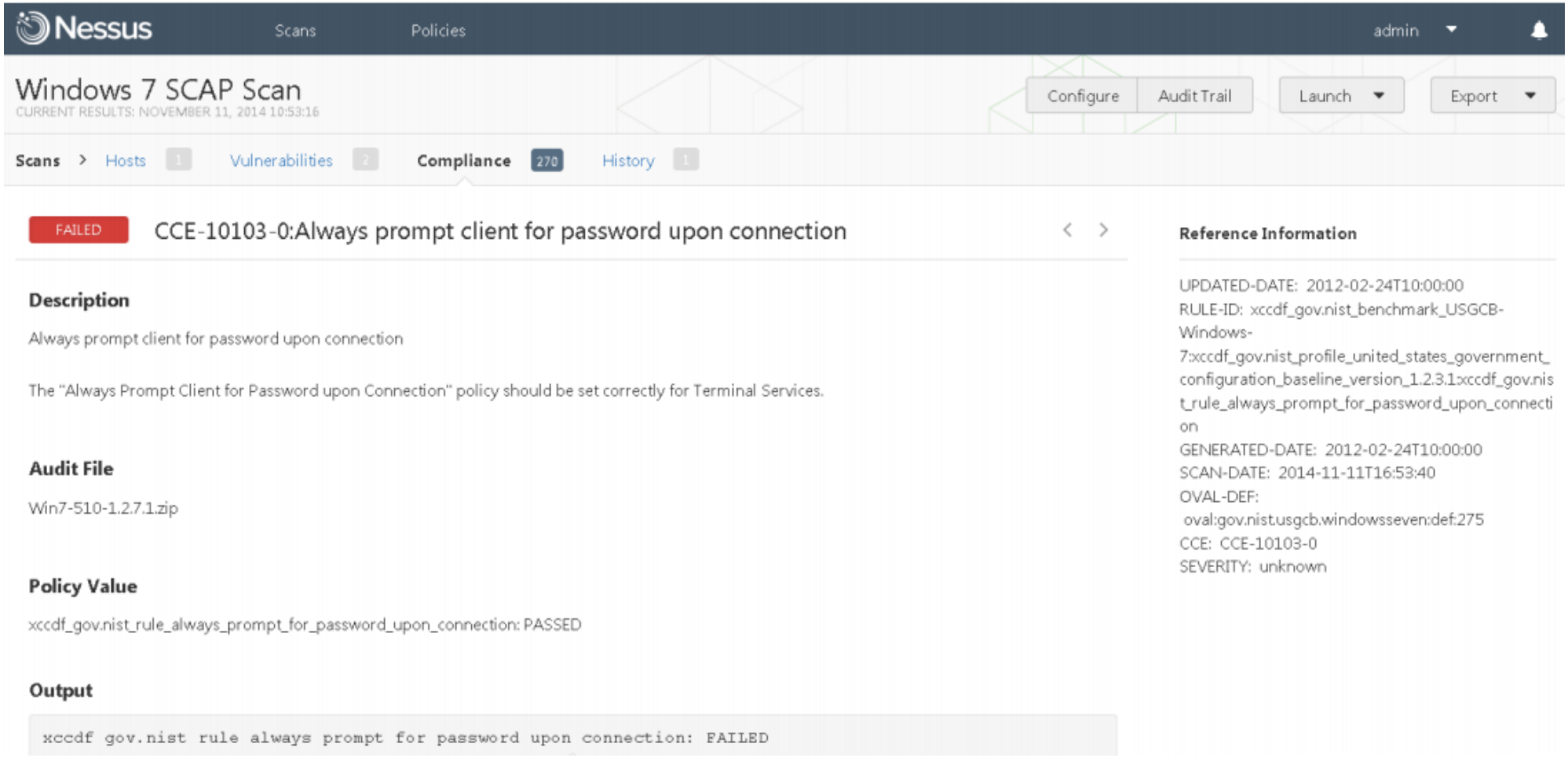
SCAP Audit Summary - Network Summary

IP Address	Score	Info	Medium	High	Total
10.31.104.0/24		1811	80	7	179	266
172.26.48.0/24		1322	101	34	122	257

SCAP Compliance Scan Results

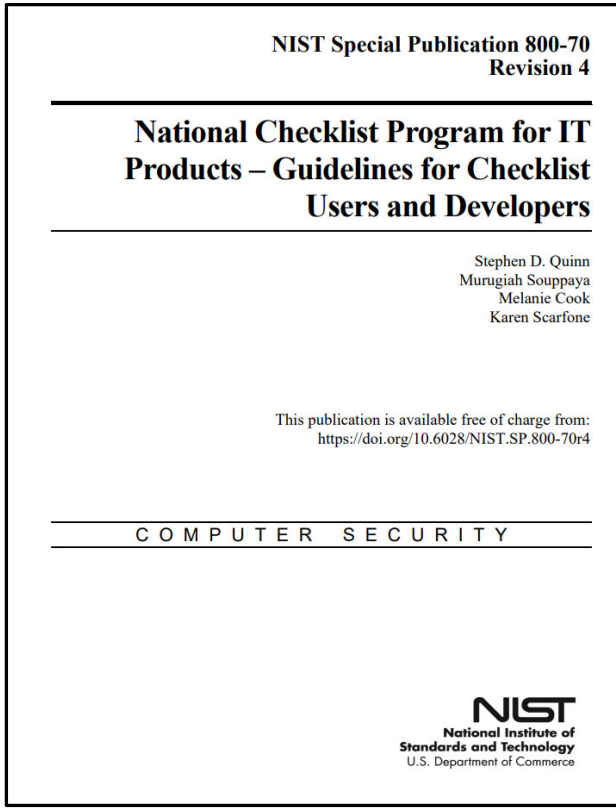


SCAP: Individual compliance check result for scanned host



SCAP (Security Content Automation Protocol) validated tools may be used to automate collection of assessment objects

- National Vulnerability Database (NVD): https://nvd.nist.gov/
- NVD SCAP Download: http://nvd.nist.gov/download.cfm
- National Checklist Program (NCP): http://web.nvd.nist.gov/view/ncp/repository
- NIST SP 800-126r3, The Technical Specification for SCAP
- NIST SP 800-70r4, National Checklist Program for IT Products
- More documentation and tools: https://scap.nist.gov/revision/1.0/index.html



NIST Special Publication 800-70
Revision 4

National Checklist Program for IT Products – Guidelines for Checklist Users and Developers

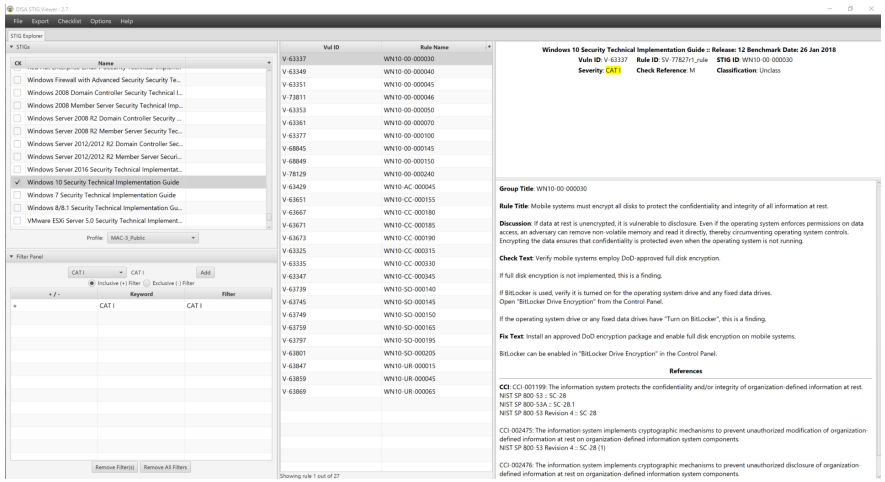
Stephen D. Quinn
Murugiah Souppaya
Melanie Cook
Karen Scarfone

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-70r4

COMPUTER SECURITY

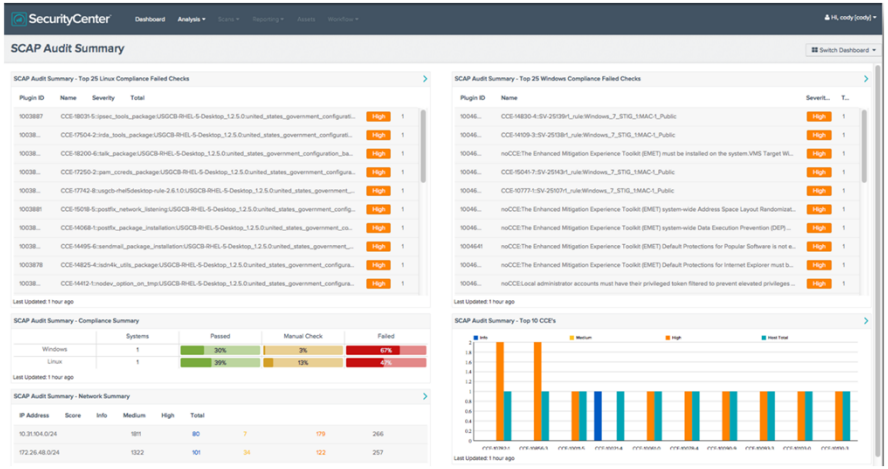
NIST
National Institute of Standards and Technology
U.S. Department of Commerce

DISA STIG Tool



+

SCAP Tool



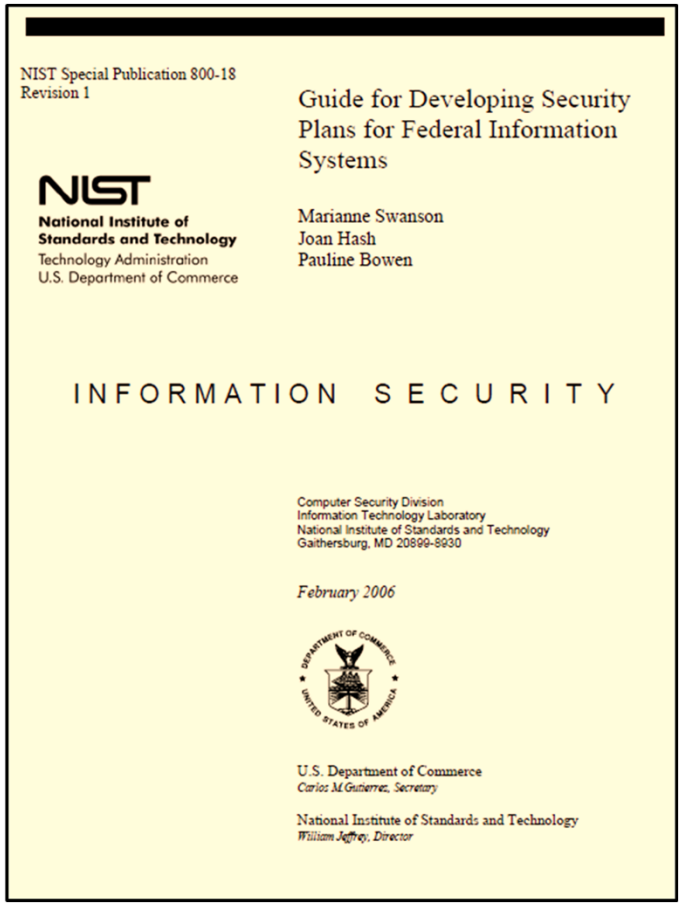
SCAP Compliance Checker

The SCAP Compliance Checker is an automated compliance scanning tool that leverages the DISA Security Technical Implementation Guidelines (STIGs) and operating system (OS) specific baselines to analyze and report on the security configuration of an information system. The tool can be run locally on the host system to be scanned, or scans can be conducted across a network from any machine on the domain. In either scanning environment, the following requirement applies: The user conducting the scan must have administrative privileges on the machine to be scanned. If the machine to be scanned is not hosting the tool, domain-level administrative privileges (or individual local administrator accounts) are required to remotely scan other systems on the network.

Agenda

- ✓Risk Management Framework – A quick review…
- ✓Implementing controls – Host hardening…
  - ✓Security configuration checklist (w/DISA STIG Viewer)
- ✓SCAP - Security Content Automation Protocol
- System Security Plan's Section 13
  - ***Select 1 technical control family or CM control family to fill out for your information system's SSP***
- Team Project - SSP draft development questions & answers…

SSP's Technical Controls: Section 13



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

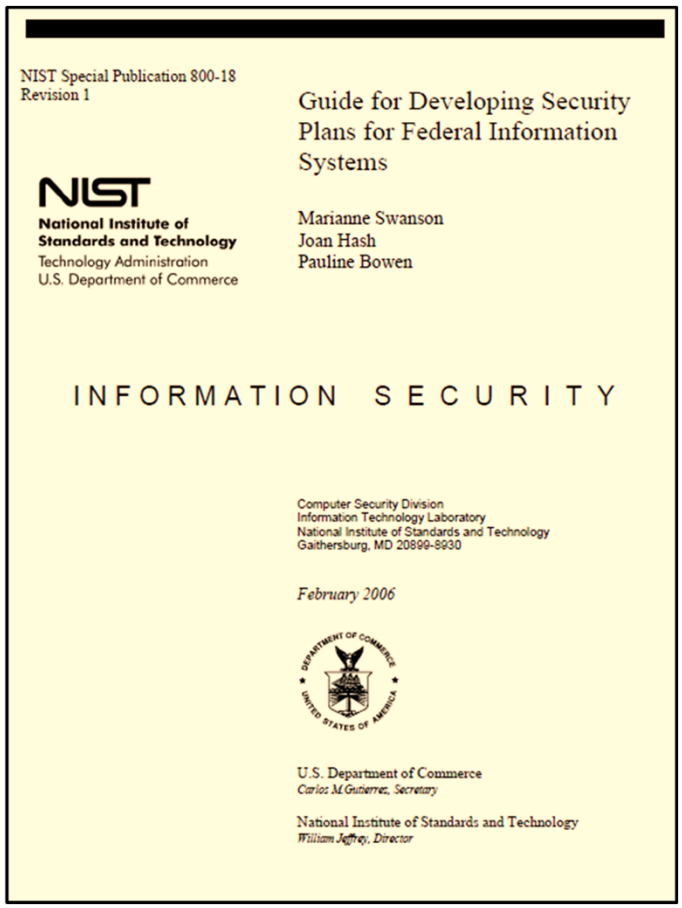
National Institute of Standards and Technology
William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Table 2: Security Control Class, Family, and Identifier

SSP – Table of Contents

Technical Controls



NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

February 2006

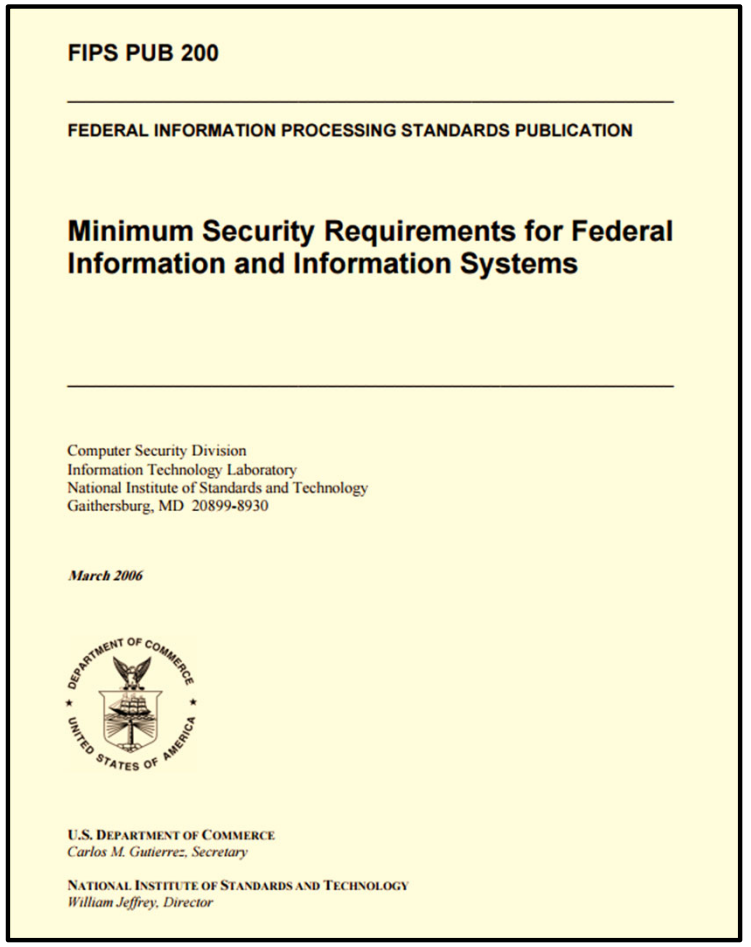
U.S. Department of Commerce
Carlos M.Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director

CLASS	FAMILY	IDENTIFIER
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Identification and Authentication (IA)

Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.



FIPS PUB 200

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Minimum Security Requirements for Federal Information and Information Systems

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

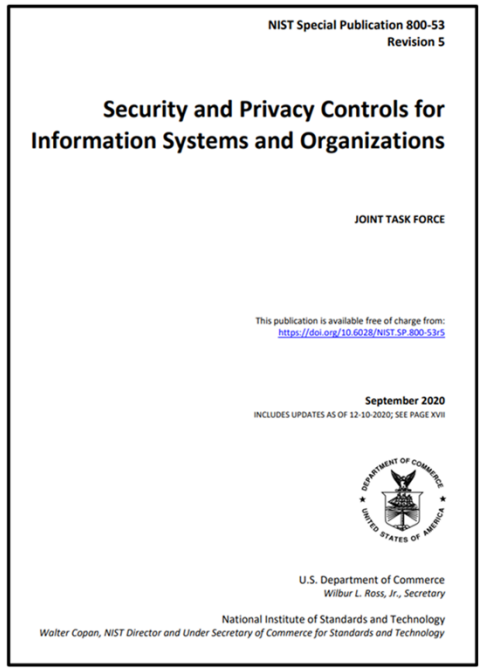
March 2006

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
William Jeffrey, Director

Identification and Authentication (IA)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)



NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

IA-1 Identification and Authentication Policy and Procedures

Control: The organization:

a. Develops, documents, and disseminates to **[*Assignment: organization-defined personnel or roles*]:**
    1. An identification and authentication policy that addresses **purpose**, **scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance**; and
    2. **Procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls**; and

b. Reviews and updates the current:
    a. Identification and authentication policy **[*Assignment: organization-defined frequency*]**; and
    b. Identification and authentication procedures **[*Assignment: organization-defined frequency*]**.

IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES			
	ASSESSMENT OBJECTIVE: *Determine if the organization:*			
	IA-1(a)(1)	**IA-1(a)(1)[1]**	*develops and documents an identification and authentication policy that addresses:*	
			IA-1(a)(1)[1][a]	*purpose;*
			IA-1(a)(1)[1][b]	*scope;*
			IA-1(a)(1)[1][c]	*roles;*
			IA-1(a)(1)[1][d]	*responsibilities;*
			IA-1(a)(1)[1][e]	*management commitment;*
			IA-1(a)(1)[1][f]	*coordination among organizational entities;*
			IA-1(a)(1)[1][g]	*compliance;*
		IA-1(a)(1)[2]	*defines personnel or roles to whom the identification and authentication policy is to be disseminated; and*	
		IA-1(a)(1)[3]	*disseminates the identification and authentication policy to organization-defined personnel or roles;*	
	IA-1(a)(2)	**IA-1(a)(2)[1]**	*develops and documents procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls;*	
		IA-1(a)(2)[2]	*defines personnel or roles to whom the procedures are to be disseminated;*	
		IA-1(a)(2)[3]	*disseminates the procedures to organization-defined personnel or roles;*	
	IA-1(b)(1)	**IA-1(b)(1)[1]**	*defines the frequency to review and update the current identification and authentication policy;*	
		IA-1(b)(1)[2]	*reviews and updates the current identification and authentication policy with the organization-defined frequency; and*	
	IA-1(b)(2)	**IA-1(b)(2)[1]**	*defines the frequency to review and update the current identification and authentication procedures; and*	
		IA-1(b)(2)[2]	*reviews and updates the current identification and authentication procedures with the organization-defined frequency.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Identification and authentication policy and procedures; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with identification and authentication responsibilities; organizational personnel with information security responsibilities].			

NIST Special Publication 800-53A
Revision 5

Assessing Security and Privacy Controls in Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53Ar5

January 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

IA-1 Identification and Authentication Policy and Procedures

NIST Special Publication 800-63-3

Digital Identity Guidelines

Paul A. Grassi
Michael E. Garcia
Applied Cybersecurity Division
Information Technology Laboratory

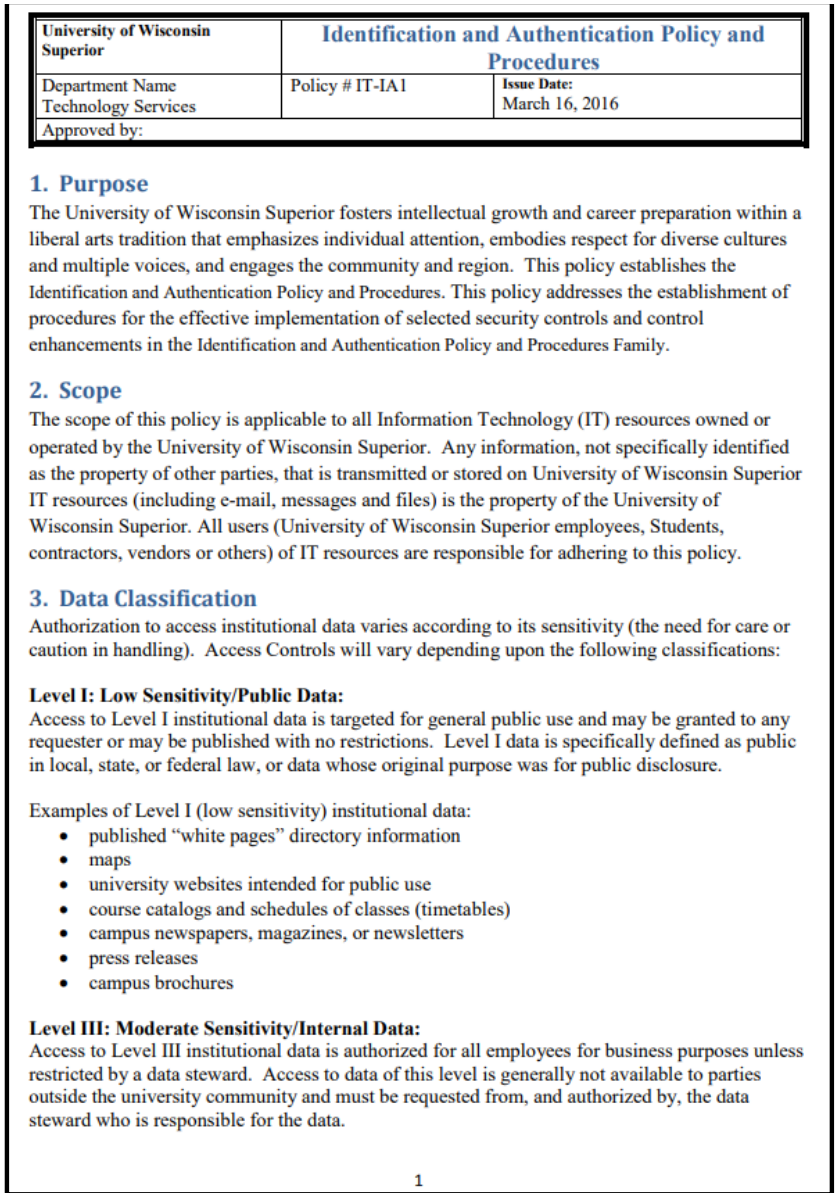
James L. Fenton
Almode Networks
Los Altos, Calif.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63-3

June 2017
INCLUDES UPDATES AS OF 12-01-2017; PAGE X

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Kent Rochford, Acting NIST Director and Under Secretary of Commerce for Standards and Technology



University of Wisconsin Superior	Identification and Authentication Policy and Procedures	
Department Name Technology Services	Policy # IT-IA1	**Issue Date:** March 16, 2016
Approved by:		

1. Purpose

The University of Wisconsin Superior fosters intellectual growth and career preparation within a liberal arts tradition that emphasizes individual attention, embodies respect for diverse cultures and multiple voices, and engages the community and region. This policy establishes the Identification and Authentication Policy and Procedures. This policy addresses the establishment of procedures for the effective implementation of selected security controls and control enhancements in the Identification and Authentication Policy and Procedures Family.

2. Scope

The scope of this policy is applicable to all Information Technology (IT) resources owned or operated by the University of Wisconsin Superior. Any information, not specifically identified as the property of other parties, that is transmitted or stored on University of Wisconsin Superior IT resources (including e-mail, messages and files) is the property of the University of Wisconsin Superior. All users (University of Wisconsin Superior employees, Students, contractors, vendors or others) of IT resources are responsible for adhering to this policy.

3. Data Classification

Authorization to access institutional data varies according to its sensitivity (the need for care or caution in handling). Access Controls will vary depending upon the following classifications:

Level I: Low Sensitivity/Public Data:
Access to Level I institutional data is targeted for general public use and may be granted to any requester or may be published with no restrictions. Level I data is specifically defined as public in local, state, or federal law, or data whose original purpose was for public disclosure.

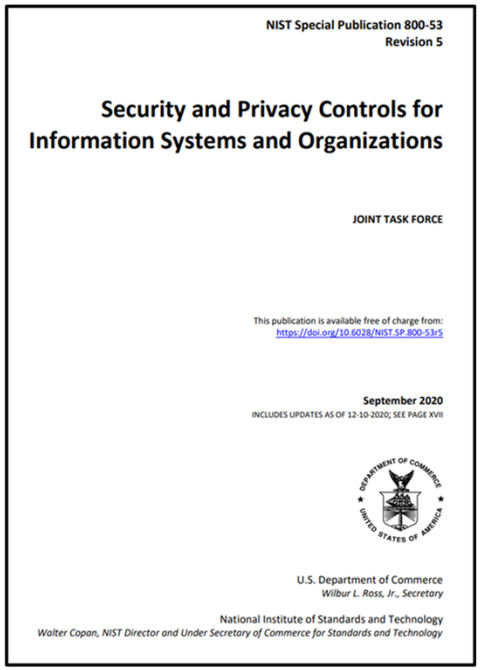
Examples of Level I (low sensitivity) institutional data:

- published "white pages" directory information
- maps
- university websites intended for public use
- course catalogs and schedules of classes (timetables)
- campus newspapers, magazines, or newsletters
- press releases
- campus brochures

Level III: Moderate Sensitivity/Internal Data:
Access to Level III institutional data is authorized for all employees for business purposes unless restricted by a data steward. Access to data of this level is generally not available to parties outside the university community and must be requested from, and authorized by, the data steward who is responsible for the data.

Identification and Authentication (IA)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
Identification and Authentication					
IA-1	Identification and Authentication Policy and Procedures	P1	IA-1	IA-1	IA-1
IA-2	Identification and Authentication (Organizational Users)	P1	IA-2 (1) (12)	IA-2 (1) (2) (3) (8) (11) (12)	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)
IA-3	Device Identification and Authentication	P1	Not Selected	IA-3	IA-3
IA-4	Identifier Management	P1	IA-4	IA-4	IA-4
IA-5	Authenticator Management	P1	IA-5 (1) (11)	IA-5 (1) (2) (3) (11)	IA-5 (1) (2) (3) (11)
IA-6	Authenticator Feedback	P2	IA-6	IA-6	IA-6
IA-7	Cryptographic Module Authentication	P1	IA-7	IA-7	IA-7
IA-8	Identification and Authentication (Non-Organizational Users)	P1	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)	IA-8 (1) (2) (3) (4)


NIST Special Publication 800-53
Revision 5

Security and Privacy Controls for Information Systems and Organizations

JOINT TASK FORCE

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-53r5

September 2020
INCLUDES UPDATES AS OF 12-10-2020; SEE PAGE XVII

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary of Commerce for Standards and Technology

A-2 *is a common control to all baselines*

IA-2 Identification and Authentication (Organizational Users)

Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users)

IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
	ASSESSMENT OBJECTIVE: *Determine if the information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system operations responsibilities; organizational personnel with information security responsibilities; system/network administrators; organizational personnel with account management responsibilities; system developers]. **Test**: [*SELECT FROM:* Organizational processes for uniquely identifying and authenticating users; automated mechanisms supporting and/or implementing identification and authentication capability].

TABLE OF CONTENTS

	Assurance Level		
Impact Categories	**1**	**2**	**3**
Inconvenience, distress or damage to standing or reputation	Low	Mod	High
Financial loss or agency liability	Low	Mod	High
Harm to agency programs or public interests	N/A	Low/Mod	High
Unauthorized release of sensitive information	N/A	Low/Mod	High
Personal Safety	N/A	Low	Mod/High
Civil or criminal violations	N/A	Low/Mod	High

Business Area	Business Area ID	Information Type	Inconvenience, distress or damage to standing or reputation	Financial loss or agency liability	Harm to agency programs or public interests	Unauthorized release of sensitive information	Personal Safety	Civil or criminal violations	IAL	AAL
Environmental Management	D.8	Pollution Prevention and Control	Low	Low	Low	Low	Low	Low		
Public Goods Creation & Management	D.22	Public Resources, Facility and Infrastructure Management	Moderate	Low	Low	Moderate	Low	Low		
		Tenant Data	***Moderate***	***Low***	***Low***	***Moderate***	***Low***	***Low***		
Information & Technology Management	C.3.5.5	Information Security	Moderate	Low	Moderate	Moderate	Low	Low		
Information & Technology Management	C.3.5.6	Record Retention	Moderate	Low	Moderate	Moderate	Low	Low		
Information & Technology Management	C.3.5.7	Information Management	Moderate	Low	Moderate	Moderate	Low	Low	*2*	*2*
Information & Technology Management	C.3.5	System and Network Monitoring	Moderate	Low	Moderate	Moderate	Low	Low		
		System Data	***Moderate***	***Low***	***Moderate***	***Moderate***	***Low***	***Low***		
			Moderate	***Low***	***Moderate***	***Moderate***	***Low***	***Low***		
		Assurance Level:	***2***	***1***	***2***	***2***	***2***	***2***		

2.3. Digital Identity Determination

The digital identity information may be found in Attachment 3, Digital Identity Worksheet.

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels co e-Authentication Level ction being performed.

The digital identity level is Choose an item.

Choose an item.
Level 1: AAL1, IAL1, FAL1
Level 2: AAL2, IAL2, FAL2
Level 3: AAL3, IAL3, FAL3

2.3. Digital Identity Determination

The digital identity information may be found in Attachment 3, Digital Identity Worksheet.

Note: NIST SP 800-63-3, Digital Identity Guidelines, does not recognize the four Levels of Assurance model previously used by federal agencies and described in OMB M-04-04, instead requiring agencies to individually select levels co e-Authentication Level ction being performed.

The digital identity level is Level 2: AAL2, IAL2, FAL2

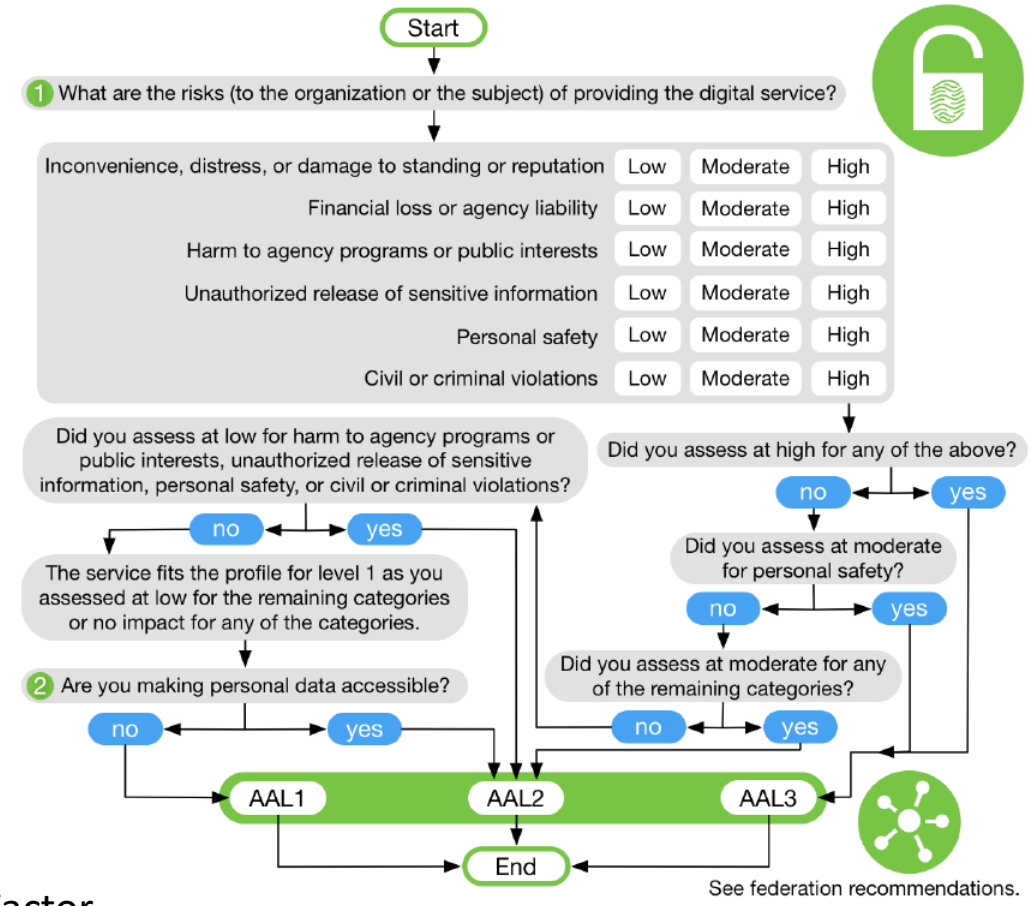
IA-2 Identification and Authentication

Control Enhancement:

IA-2(1)	IDENTIFICATION AND AUTHENTICATION | *NETWORK ACCESS TO PRIVILEGED ACCOUNTS*
	ASSESSMENT OBJECTIVE: *Determine if the information system implements multifactor authentication for network access to privileged accounts.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing user identification and authentication; information system design documentation; information system configuration settings and associated documentation; information system audit records; list of information system accounts; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with information system operations responsibilities; organizational personnel with account management responsibilities; organizational personnel with information security responsibilities; system/network administrators; system developers]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing multifactor authentication capability].

Authenticator Assurance

Requirement	AAL1	AAL2	AAL3
Permitted Authenticator Types	Memorized Secret; Look-Up Secret; Out-of-Band; SF OTP Device; MF OTP Device; SF Crypto Software; SF Crypto Device; MF Crypto Software; MF Crypto Device	MF OTP Device; MF Crypto Software; MF Crypto Device; or Memorized Secret plus: • Look-Up Secret • Out-of-Band • SF OTP Device • SF Crypto Software • SF Crypto Device	MF Crypto Device; SF Crypto Device plus Memorized Secret; SF OTP Device plus MF Crypto Device or Software; SF OTP Device plus SF Crypto Software plus Memorized Secret
FIPS 140 Verification	Level 1 (Government agency verifiers)	Level 1 (Government agency authenticators and verifiers)	Level 2 overall (MF authenticators) Level 1 overall (verifiers and SF Crypto Devices) Level 3 physical security (all authenticators)
Reauthentication	30 days	12 hours or 30 minutes inactivity; MAY use one authentication factor	12 hours or 15 minutes inactivity; SHALL use both authentication factors
Security Controls	SP 800-53 Low Baseline (or equivalent)	SP 800-53 Moderate Baseline (or equivalent)	SP 800-53 High Baseline (or equivalent)
MitM Resistance	Required	Required	Required
Verifier-Impersonation Resistance	Not required	Not required	Required
Verifier-Compromise Resistance	Not required	Not required	Required
Replay Resistance	Not required	Not required	Required
Authentication Intent	Not required	Recommended	Required
Records Retention Policy	Required	Required	Required
Privacy Controls	Required	Required	Required



AAL1 : = 1 Factor

AAL2 : = 2 Factors

AAL3 : = 2 Factors: Hardware-based authenticator and an authenticator that provides verifier impersonation resistance

AAL = Authenticator Assurance Level

Agenda

- ✓NIST Risk Management Framework – A quick review…
- ✓Implementing controls – Host hardening…
  - ✓Security configuration checklist (w/DISA STIG Viewer)
- ✓NIST 800-53Ar4 – How Controls are Assessed
- ✓SCAP - Security Content Automation Protocol
- ✓FedRAMP System Security Plan's Section 13 – A controls deep dive
  - ✓Identity and Authentication – controls assessment questions
- Team Project - SSP drafts…

SSP – Table of Contents

8.1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

Question (Yes/No)	Conclusion
Does the system use virtual machines?	A no response means that system is most likely not a cloud.
Does the system have the ability to expand its capacity to meet customer demand?	A no response means that the system is most likely not a cloud.
Does the system allow the consumer to build anything other than servers?	A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS.
Does the system offer the ability to create databases?	A yes response means that the system is a PaaS.
Does the system offer various developer toolkits and APIs?	A yes response means that the system is a PaaS.
Does the system offer only applications that are available by obtaining a login?	A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS.

The layers of the Enter Information System Abbreviation defined in this SSP are indicated in Table 8-1. Service Layers Represented in this SSP that follows.

Table 8-1. Service Layers Represented in this SSP

Service Provider Architecture Layers		
☐	Software as a Service (SaaS)	Major Application
☐	Platform as a Service (PaaS)	Major Application
☐	Infrastructure as a Service (IaaS)	General Support System
☐	Other	Explain: Click here to enter text.

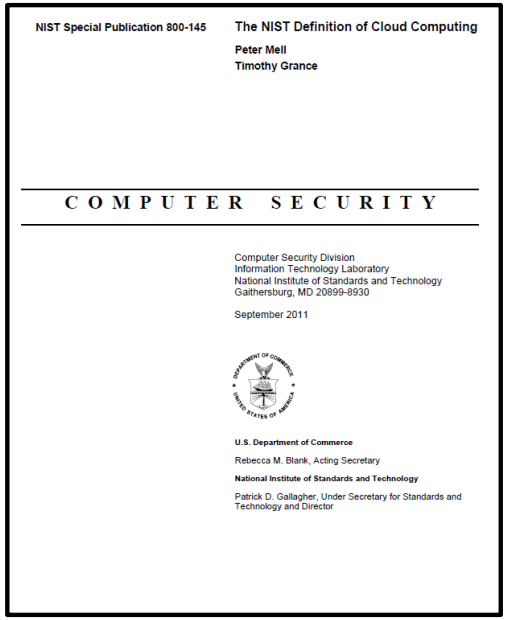
Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

8.2. Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the Enter Information System Abbreviation that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8-2. Cloud Deployment Model Represented in this SSP that follows.

Table 8-2. Cloud Deployment Model Represented in this SSP

Service Provider Cloud Deployment Model		
☐	Public	Cloud services and infrastructure supporting multiple organizations and agency clients
☐	Private	Cloud services and infrastructure dedicated to a specific organization/agency and no other clients
☐	Government Only Community	Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations
☐	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) Click here to enter text.



NIST Special Publication 800-145

The NIST Definition of Cloud Computing

Peter Mell
Timothy Grance

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

September 2011

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary
National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary for Standards and Technology and Director

Essential Characteristics of Cloud Computing

1. **On-demand self-service**

   A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider

2. **Broad network access**

   Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations)

3. **Resource pooling**

   The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth

4. **Rapid elasticity**

   Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time

5. **Measured service**

   Cloud systems automatically control and optimize resource use by leveraging a metering capability (typically done on pay-per-use or charge-per-use basis) at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service

Cloud Service Models

Infrastructure as a Service (IaaS)

- The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications
- The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls)

Platform as a Service (PaaS)

- The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment

Software as a Service (SaaS)

- The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface
- The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited userspecific application configuration settings

8.1. Cloud Service Models

Information systems, particularly those based on cloud architecture models, are made up of different service layers. Below are some questions that help the system owner determine if their system is a cloud followed by specific questions to help the system owner determine the type of cloud.

Question (Yes/No)	Conclusion
Does the system use virtual machines?	A no response means that system is most likely not a cloud.
Does the system have the ability to expand its capacity to meet customer demand?	A no response means that the system is most likely not a cloud.
Does the system allow the consumer to build anything other than servers?	A no response means that the system is an IaaS. A yes response means that the system is either a PaaS or a SaaS.
Does the system offer the ability to create databases?	A yes response means that the system is a PaaS.
Does the system offer various developer toolkits and APIs?	A yes response means that the system is a PaaS.
Does the system offer only applications that are available by obtaining a login?	A yes response means that system is a SaaS. A no response means that the system is either a PaaS or an IaaS.

The layers of the Enter Information System Abbreviation defined in this SSP are indicated in Table 8-1. Service Layers Represented in this SSP that follows.

Table 8-1. Service Layers Represented in this SSP

Service Provider Architecture Layers		
☐	Software as a Service (SaaS)	Major Application
☐	Platform as a Service (PaaS)	Major Application
☐	Infrastructure as a Service (IaaS)	General Support System
☐	Other	Explain: Click here to enter text.

Note: Refer to NIST SP 800-145 for information on cloud computing architecture models.

Cloud Deployment Models

Private cloud

- The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units)
- It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises

Community cloud

- The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations)
- It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises

Public cloud

- The cloud infrastructure is provisioned for open use by the general public
- It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider

Hybrid cloud

The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)

8.2. Cloud Deployment Models

Information systems are made up of different deployment models. The deployment models of the Enter Information System Abbreviation that are defined in this SSP and are not leveraged by any other FedRAMP Authorizations, are indicated in Table 8-2. Cloud Deployment Model Represented in this SSP that follows.

Table 8-2. Cloud Deployment Model Represented in this SSP

Service Provider Cloud Deployment Model		
☐	Public	Cloud services and infrastructure supporting multiple organizations and agency clients
☐	Private	Cloud services and infrastructure dedicated to a specific organization/agency and no other clients
☐	Government Only Community	Cloud services and infrastructure shared by several organizations/agencies with same policy and compliance considerations
☐	Hybrid	Explain: (e.g., cloud services and infrastructure that provides private cloud for secured applications and data where required and public cloud for other applications and data) Click here to enter text.

Agenda

- ✓NIST Risk Management Framework – A quick review…
- ✓Implementing controls – Host hardening…
  - ✓Security configuration checklist (w/DISA STIG Viewer)
- ✓NIST 800-53Ar4 – How Controls are Assessed
- ✓SCAP - Security Content Automation Protocol
- ✓FedRAMP System Security Plan's Section 13 – A controls deep dive
  - ✓Identity and Authentication – controls assessment questions
- ✓System Security Plan's Section 8
  - ✓Information System Type
- ✓Team Project - SSP drafts…