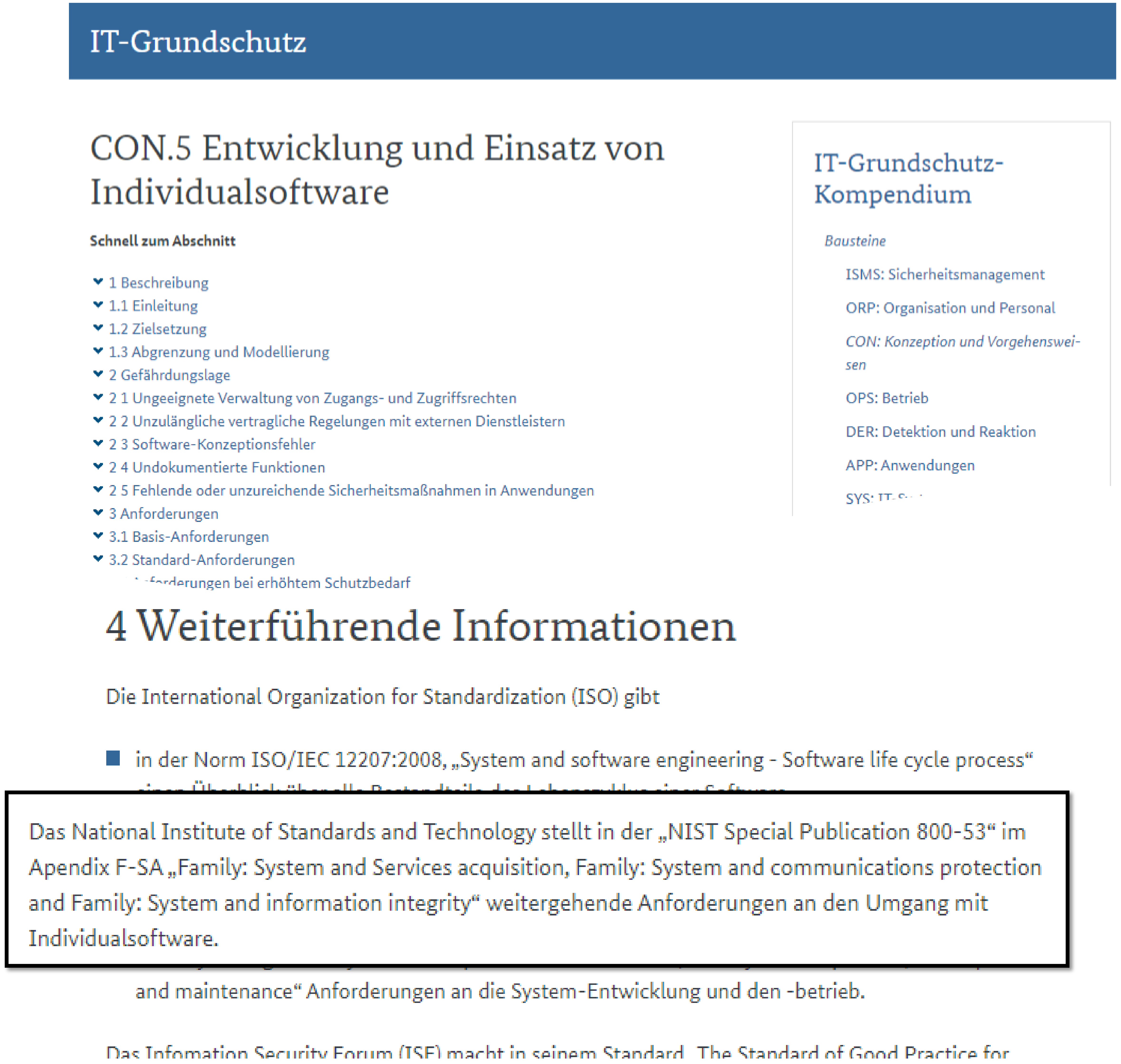
IT-Grundschutz im Rest der Welt: Cybersecurity Framework und NIST SP 800-53

A. Koderman (SerNet)

IT-Grundschutz Kompendium

CON.5:



IT-Grundschutz

CON.5 Entwicklung und Einsatz von Individualsoftware

Schnell zum Abschnitt

IT-Grundschutz-Kompendium

Bausteine

ISMS: Sicherheitsmanagement

ORP: Organisation und Personal

CON: Konzeption und Vorgehensweisen

OPS: Betrieb

DER: Detektion und Reaktion

APP: Anwendungen

SYS: IT-S

4 Weiterführende Informationen

Die International Organization for Standardization (ISO) gibt

- in der Norm ISO/IEC 12207:2008, „System and software engineering - Software life cycle process“

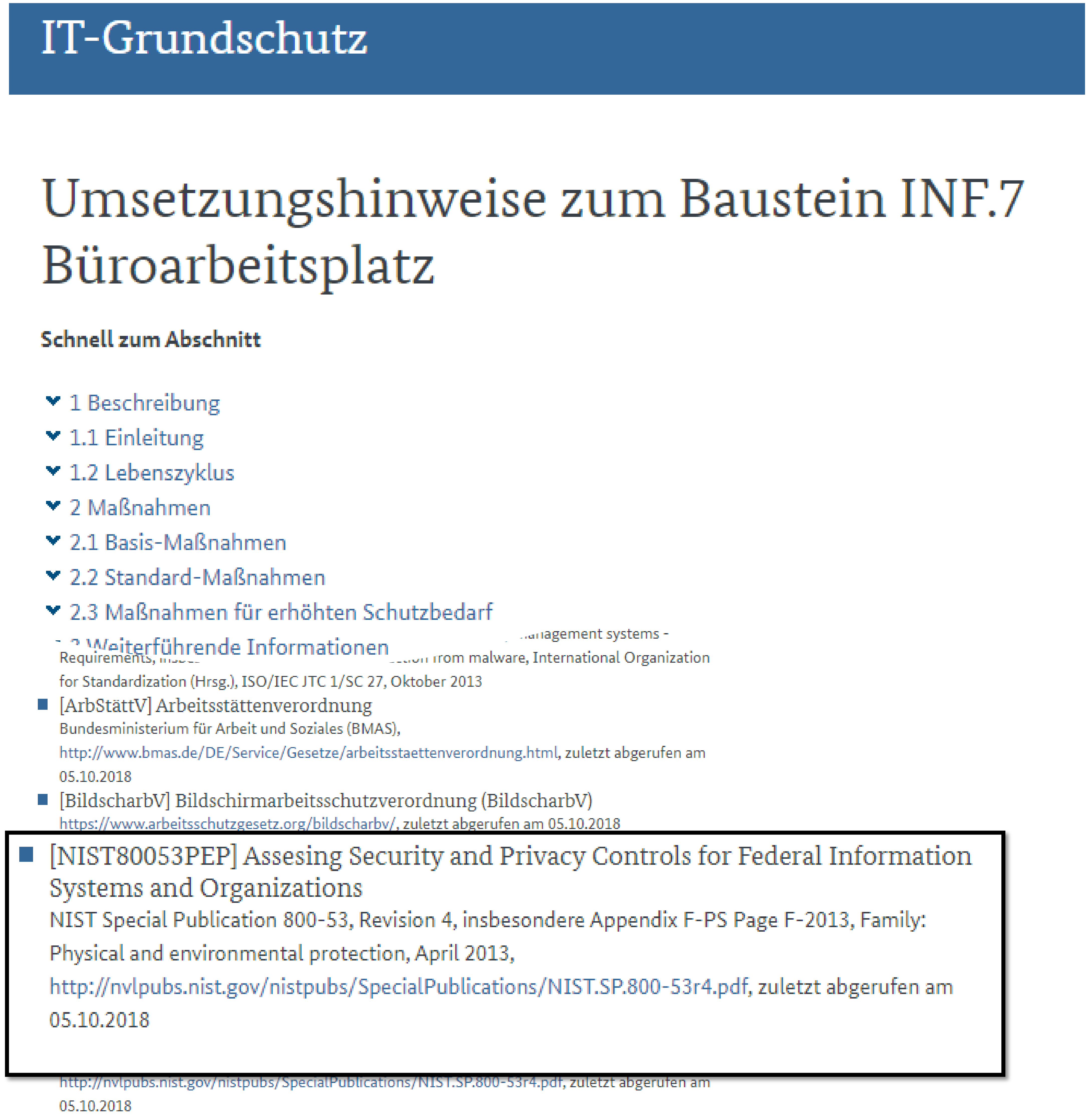
Das National Institute of Standards and Technology stellt in der „NIST Special Publication 800-53“ im Apendix F-SA „Family: System and Services acquisition, Family: System and communications protection and Family: System and information integrity“ weitergehende Anforderungen an den Umgang mit Individualsoftware.

and maintenance“ Anforderungen an die System-Entwicklung und den -betrieb.

Das Infomation Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for

IT-Grundschutz Kompendium

Umsetzungshinweise:



IT-Grundschutz

Umsetzungshinweise zum Baustein INF.7 Büroarbeitsplatz

Schnell zum Abschnitt

- 1 Beschreibung
- 1.1 Einleitung
- 1.2 Lebenszyklus
- 2 Maßnahmen
- 2.1 Basis-Maßnahmen
- 2.2 Standard-Maßnahmen
- 2.3 Maßnahmen für erhöhten Schutzbedarf
- Weiterführende Informationen

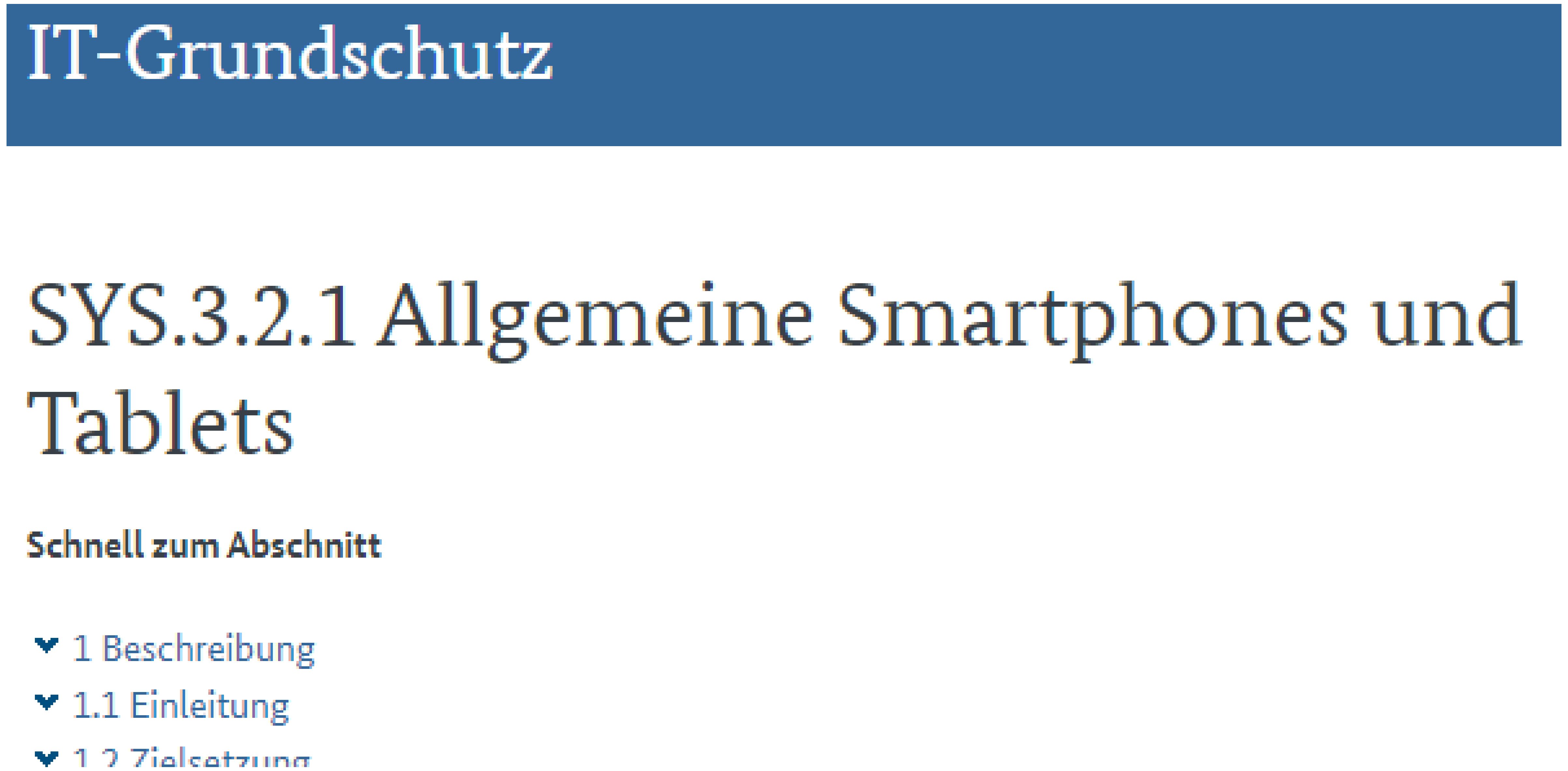
anagement systems - Requirements, from malware, International Organization for Standardization (Hrsg.), ISO/IEC JTC 1/SC 27, Oktober 2013

- [ArbStättV] Arbeitsstättenverordnung
  Bundesministerium für Arbeit und Soziales (BMAS), http://www.bmas.de/DE/Service/Gesetze/arbeitsstaettenverordnung.html, zuletzt abgerufen am 05.10.2018
- [BildscharbV] Bildschirmarbeitsschutzverordnung (BildscharbV)
  https://www.arbeitsschutzgesetz.org/bildscharbv/, zuletzt abgerufen am 05.10.2018
- [NIST80053PEP] Assesing Security and Privacy Controls for Federal Information Systems and Organizations
  NIST Special Publication 800-53, Revision 4, insbesondere Appendix F-PS Page F-2013, Family: Physical and environmental protection, April 2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, zuletzt abgerufen am 05.10.2018

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf, zuletzt abgerufen am 05.10.2018

IT-Grundschutz Kompendium

SYS.3.2.1:



IT-Grundschutz

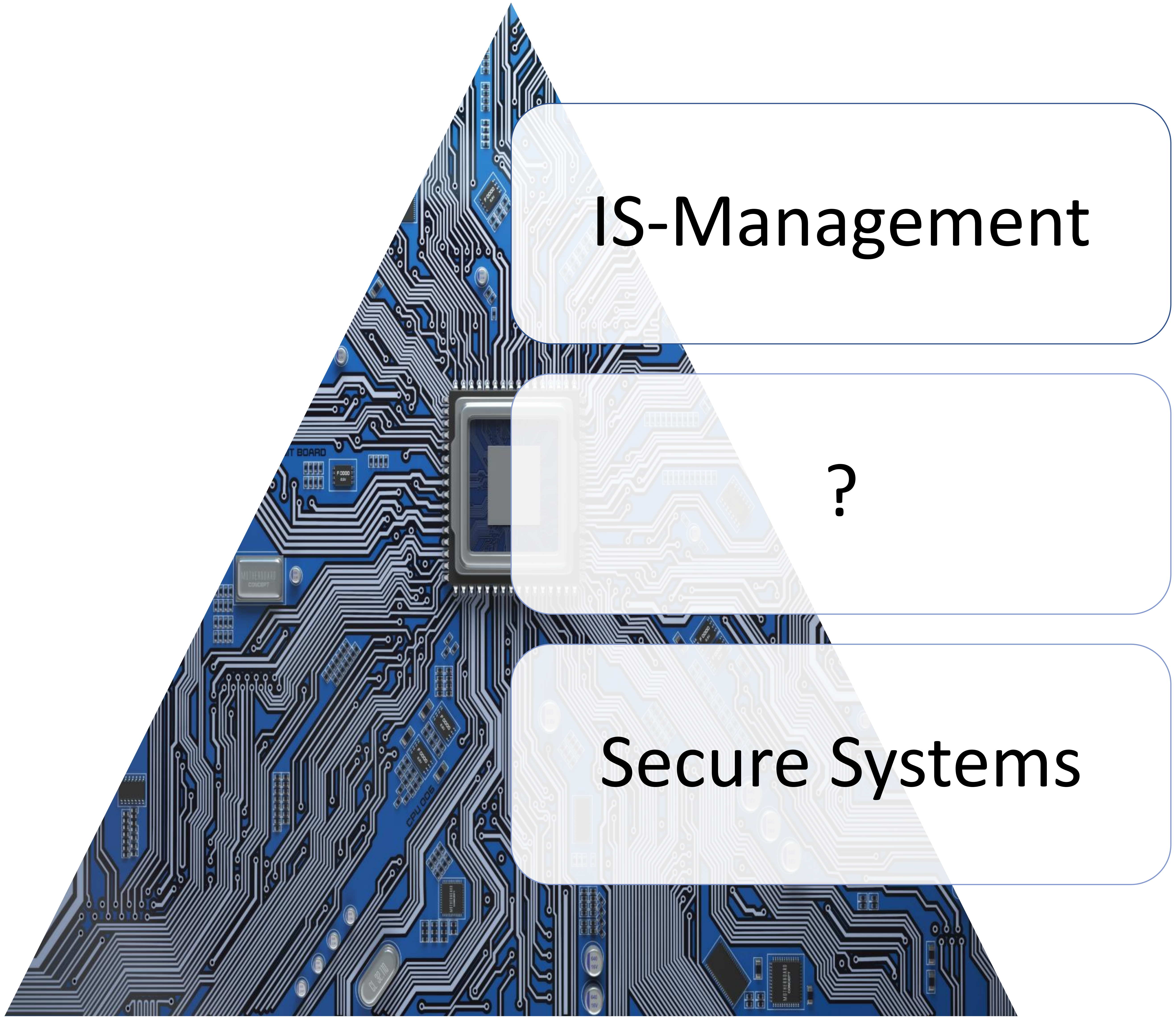
SYS.3.2.1 Allgemeine Smartphones und Tablets

Schnell zum Abschnitt

4 Weiterführende Informationen

Das National Institute of Standards and Technology (NIST) stellt folgende Dokumente im Bereich mobile Endgeräte bereit:

- „Guidelines for Managing the Security of Mobile Devices in the Enterprise: NIST Special Publication 800-124“, Revision 1, Juni 2013
- „Security and Privacy Controls for Federal Information Systems and Organizations: NIST Special Publication 800-53“, Revision 4, April 2013
- „Securing Electronic Health Record on Mobile Devices: NIST Special Publication 1800-1d“, Draft, Juli 2015

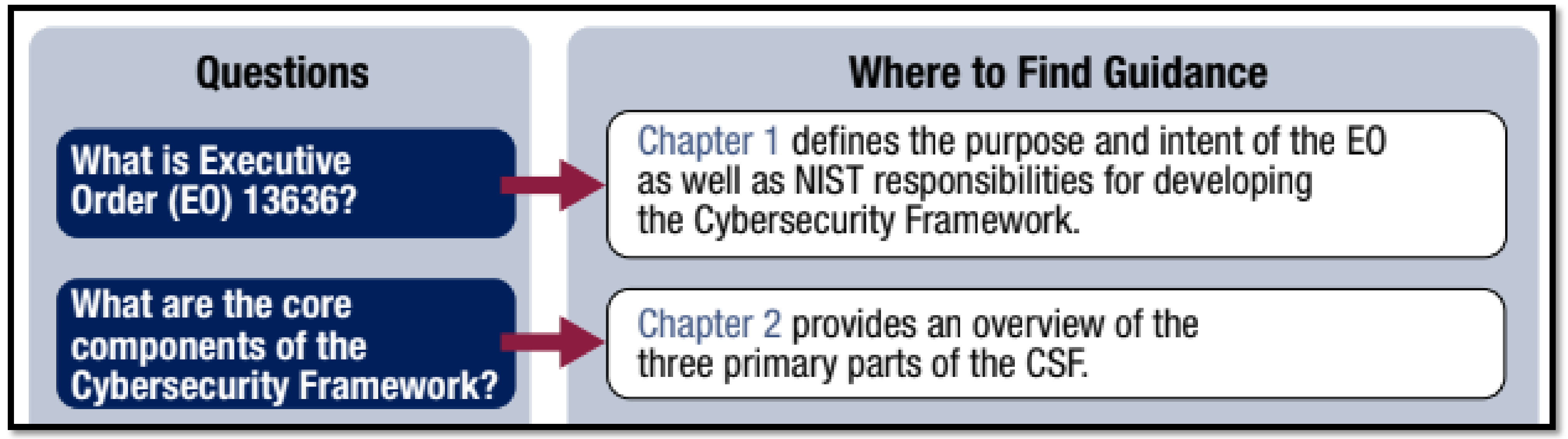


IS-Management

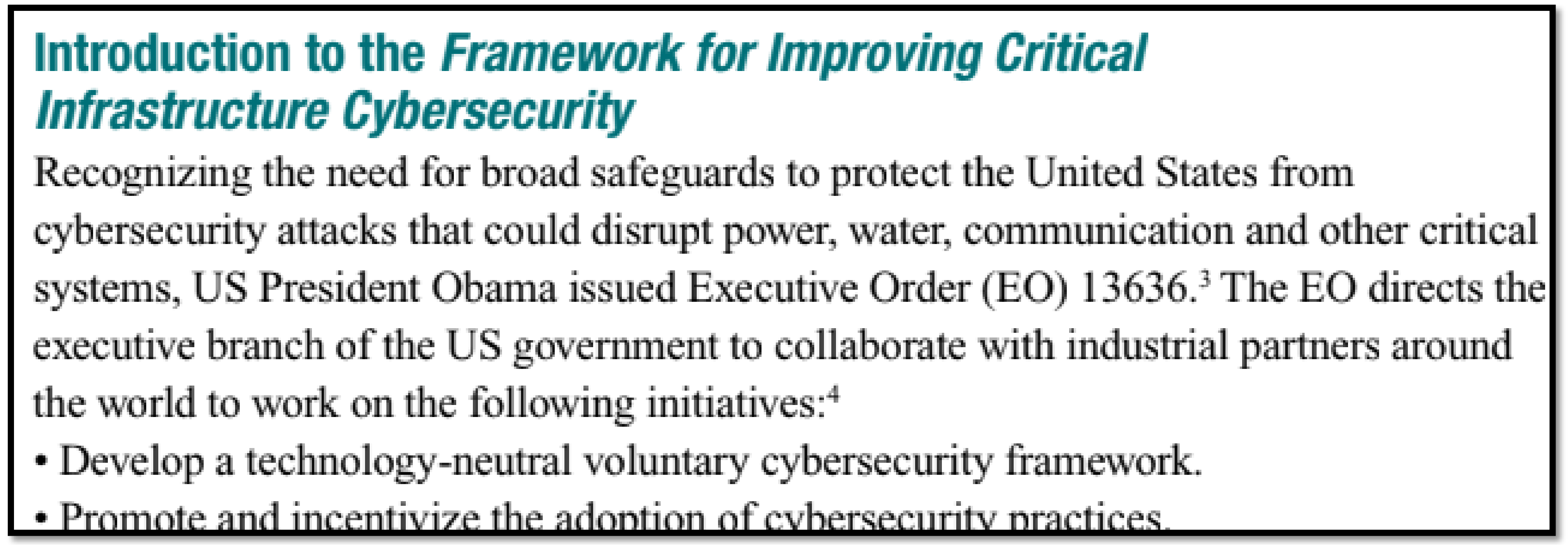
?

Secure Systems

NIST Cybersecurity Framework



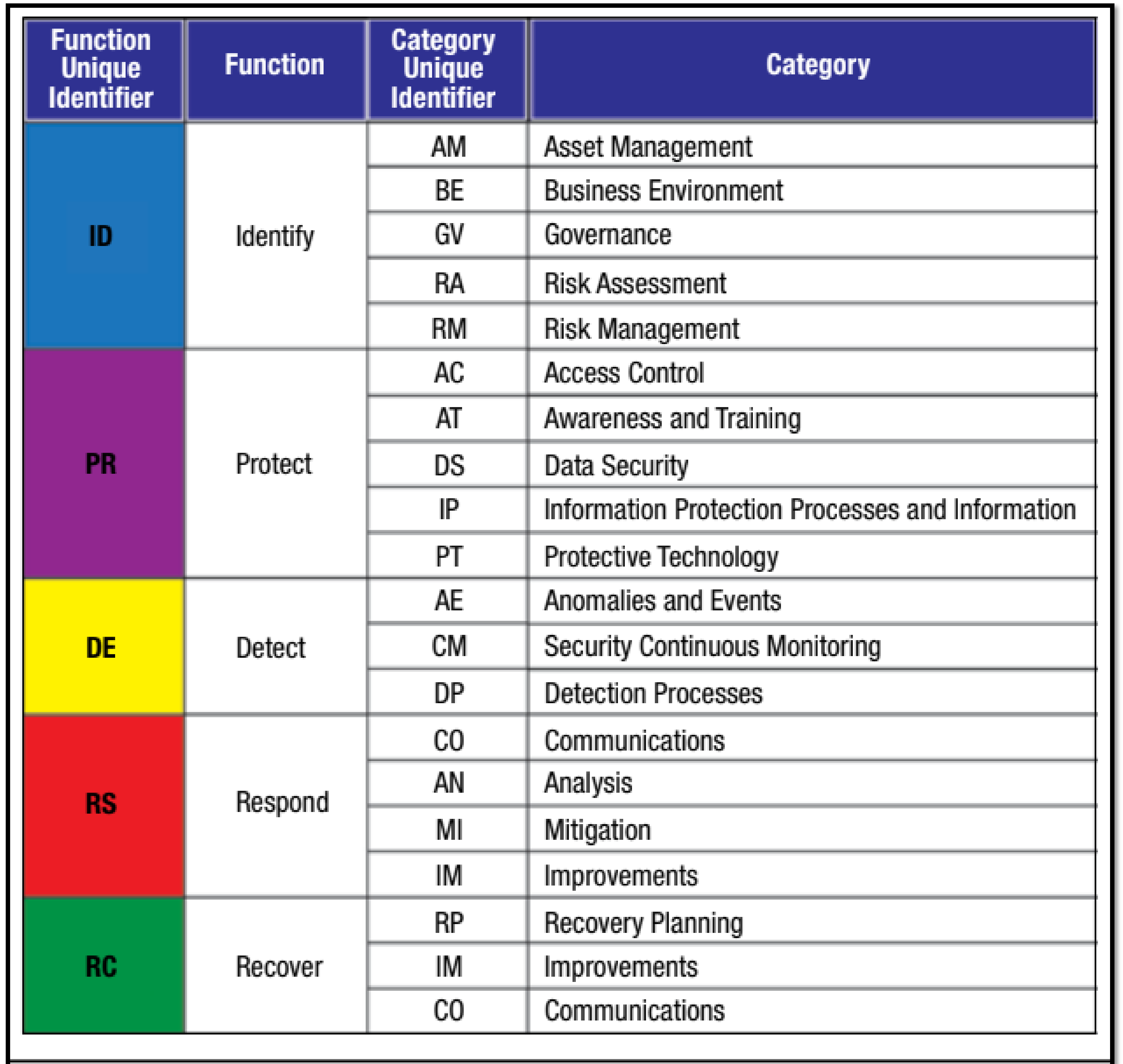
Questions	Where to Find Guidance
What is Executive Order (EO) 13636?	Chapter 1 defines the purpose and intent of the EO as well as NIST responsibilities for developing the Cybersecurity Framework.
What are the core components of the Cybersecurity Framework?	Chapter 2 provides an overview of the three primary parts of the CSF.



Introduction to the *Framework for Improving Critical Infrastructure Cybersecurity*

Recognizing the need for broad safeguards to protect the United States from cybersecurity attacks that could disrupt power, water, communication and other critical systems, US President Obama issued Executive Order (EO) 13636.[3] The EO directs the executive branch of the US government to collaborate with industrial partners around the world to work on the following initiatives:[4]

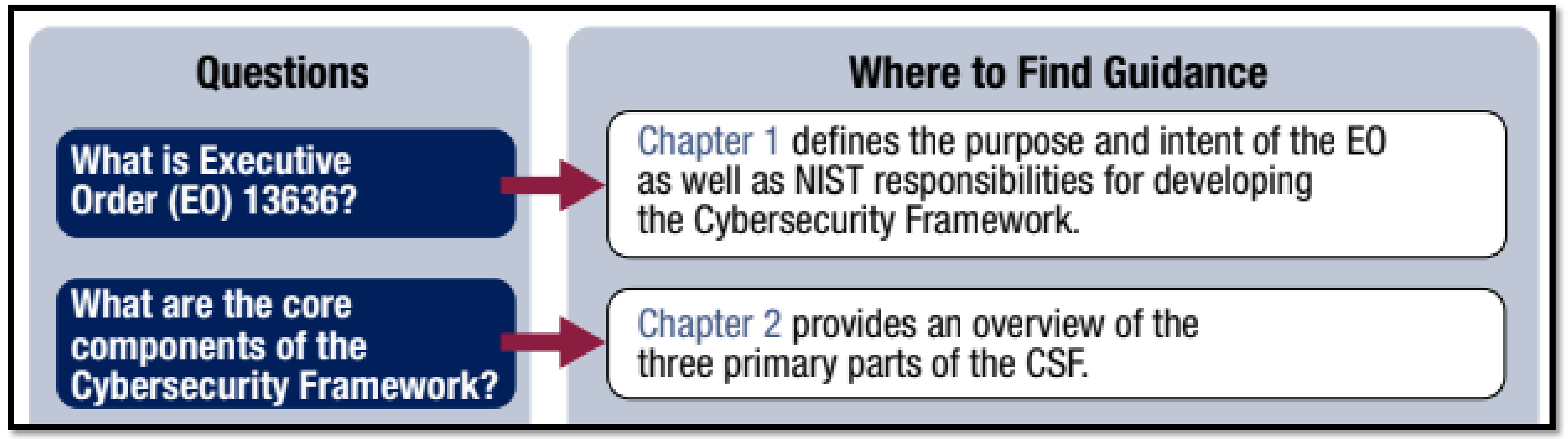
- Develop a technology-neutral voluntary cybersecurity framework.
- Promote and incentivize the adoption of cybersecurity practices.



Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Information
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Source: *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, USA, 2014, Table 1

NIST Cybersecurity Framework



Questions

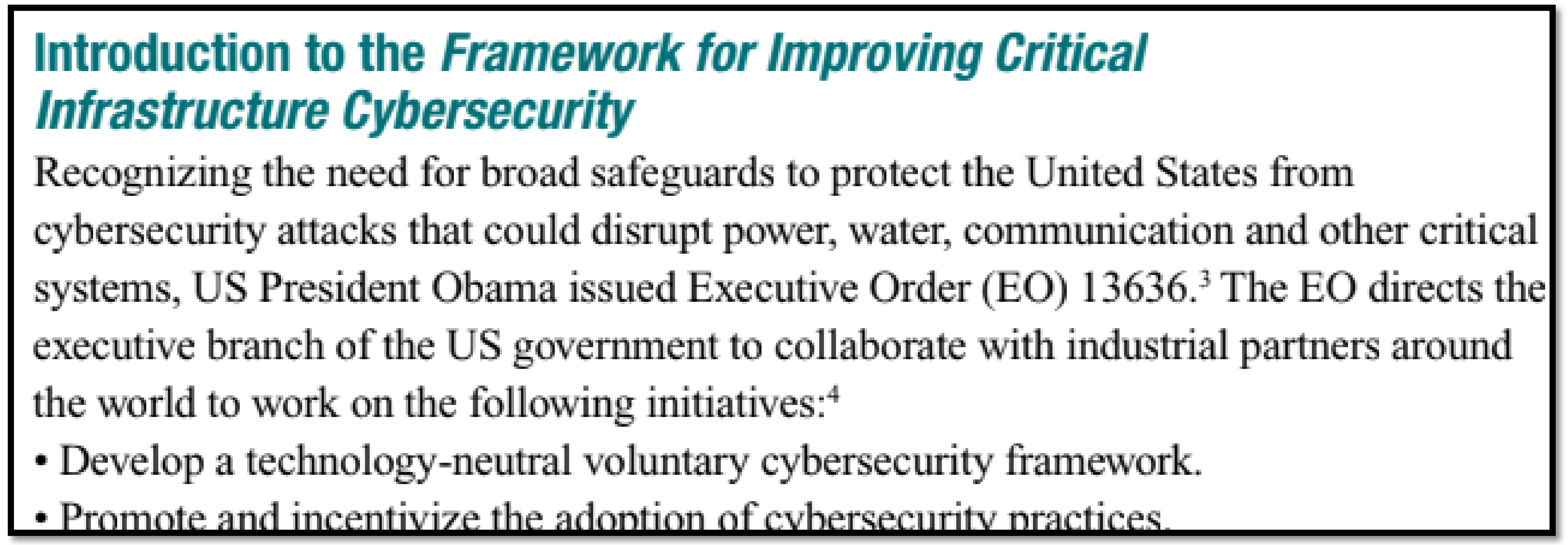
What is Executive Order (EO) 13636?

What are the core components of the Cybersecurity Framework?

Where to Find Guidance

Chapter 1 defines the purpose and intent of the EO as well as NIST responsibilities for developing the Cybersecurity Framework.

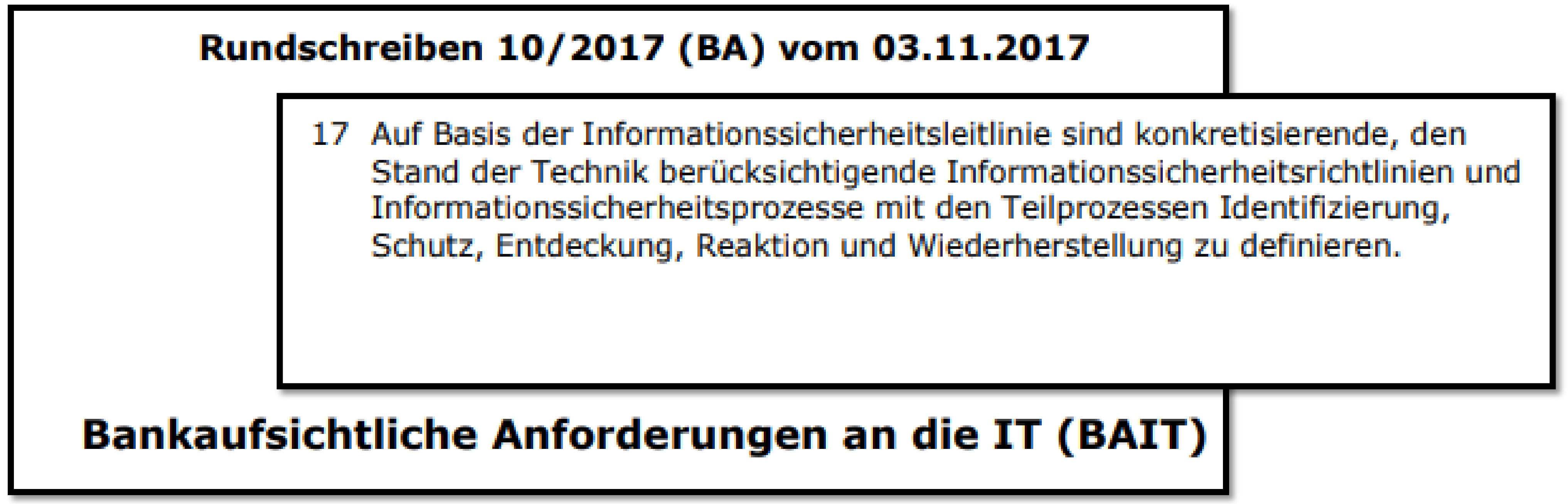
Chapter 2 provides an overview of the three primary parts of the CSF.



Introduction to the *Framework for Improving Critical Infrastructure Cybersecurity*

Recognizing the need for broad safeguards to protect the United States from cybersecurity attacks that could disrupt power, water, communication and other critical systems, US President Obama issued Executive Order (EO) 13636.[3] The EO directs the executive branch of the US government to collaborate with industrial partners around the world to work on the following initiatives:[4]

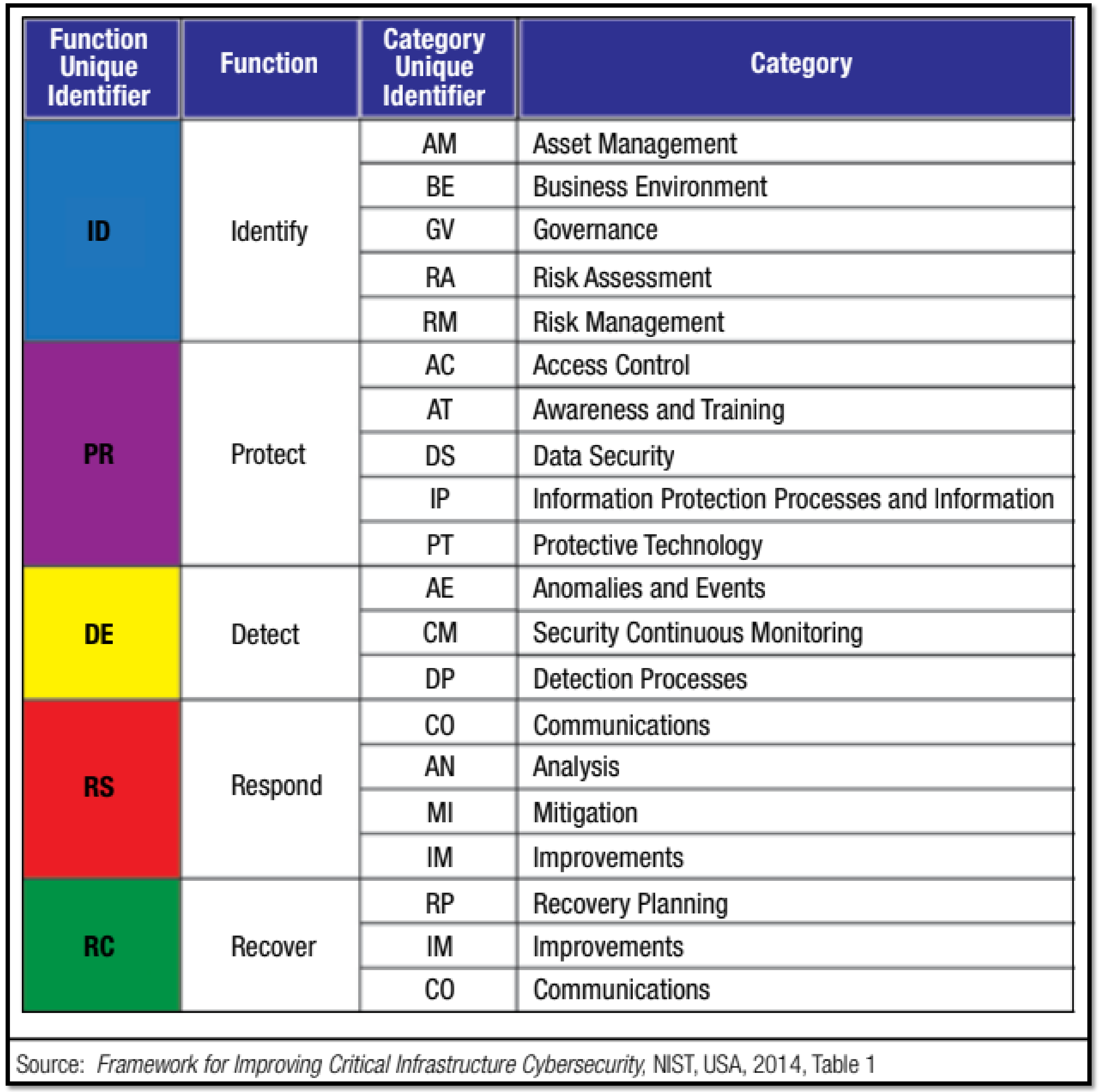
- Develop a technology-neutral voluntary cybersecurity framework.
- Promote and incentivize the adoption of cybersecurity practices.



Rundschreiben 10/2017 (BA) vom 03.11.2017

17 Auf Basis der Informationssicherheitsleitlinie sind konkretisierende, den Stand der Technik berücksichtigende Informationssicherheitsrichtlinien und Informationssicherheitsprozesse mit den Teilprozessen Identifizierung, Schutz, Entdeckung, Reaktion und Wiederherstellung zu definieren.

Bankaufsichtliche Anforderungen an die IT (BAIT)

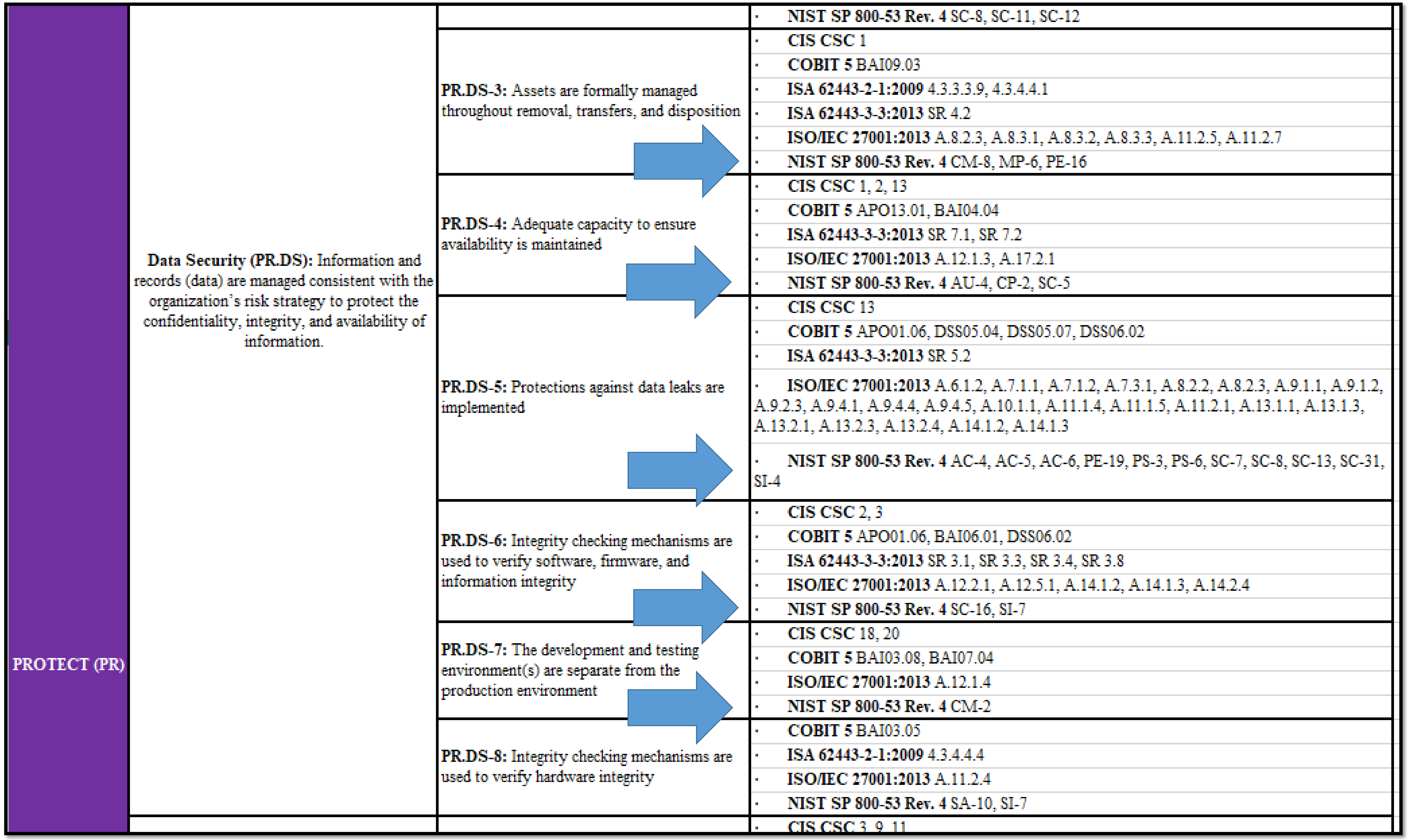


Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	AM	Asset Management
		BE	Business Environment
		GV	Governance
		RA	Risk Assessment
		RM	Risk Management
PR	Protect	AC	Access Control
		AT	Awareness and Training
		DS	Data Security
		IP	Information Protection Processes and Information
		PT	Protective Technology
DE	Detect	AE	Anomalies and Events
		CM	Security Continuous Monitoring
		DP	Detection Processes
RS	Respond	CO	Communications
		AN	Analysis
		MI	Mitigation
		IM	Improvements
RC	Recover	RP	Recovery Planning
		IM	Improvements
		CO	Communications

Source: *Framework for Improving Critical Infrastructure Cybersecurity*, NIST, USA, 2014, Table 1

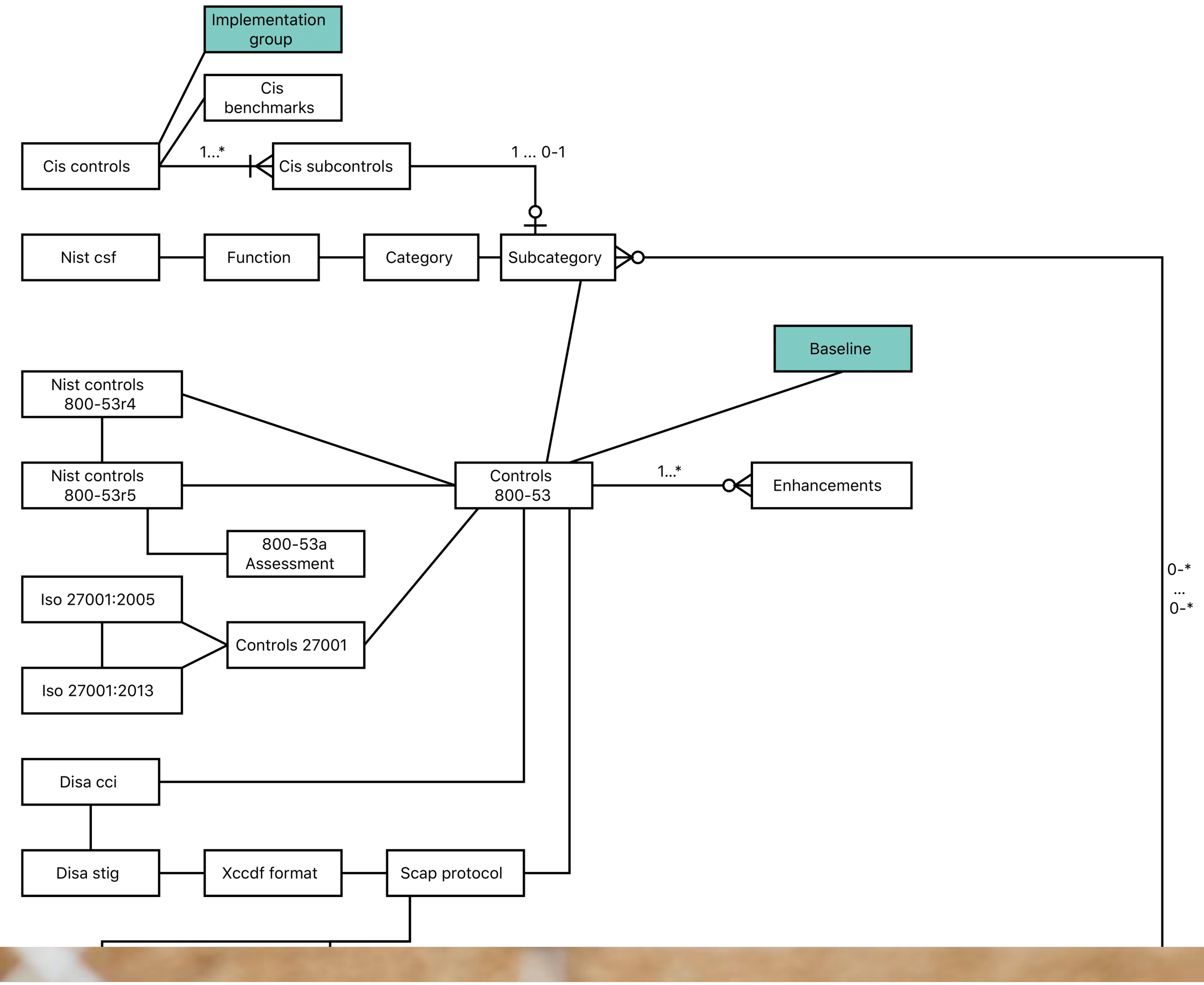
NIST Cybersecurity Framework

RECOVER
IDENTIFY
PROTECT
DETECT
RESPOND
CYBERSECURITY FRAMEWORK VERSION 1.1



PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.		· **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **CIS CSC** 1
			· **COBIT 5** BAI09.03
			· **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1
			· **ISA 62443-3-3:2013** SR 4.2
			· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7
			· **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	· **CIS CSC** 1, 2, 13
			· **COBIT 5** APO13.01, BAI04.04
			· **ISA 62443-3-3:2013** SR 7.1, SR 7.2
			· **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1
			· **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	· **CIS CSC** 13
			· **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02
			· **ISA 62443-3-3:2013** SR 5.2
			· **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
			· **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· **CIS CSC** 2, 3
			· **COBIT 5** APO01.06, BAI06.01, DSS06.02
			· **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8
			· **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4
			· **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production environment	· **CIS CSC** 18, 20
			· **COBIT 5** BAI03.08, BAI07.04
			· **ISO/IEC 27001:2013** A.12.1.4
			· **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	· **COBIT 5** BAI03.05
			· **ISA 62443-2-1:2009** 4.3.4.4.4
			· **ISO/IEC 27001:2013** A.11.2.4
			· **NIST SP 800-53 Rev. 4** SA-10, SI-7
			· **CIS CSC** 3, 9, 11

Standard-Korrelationen



NIST 800-53r4

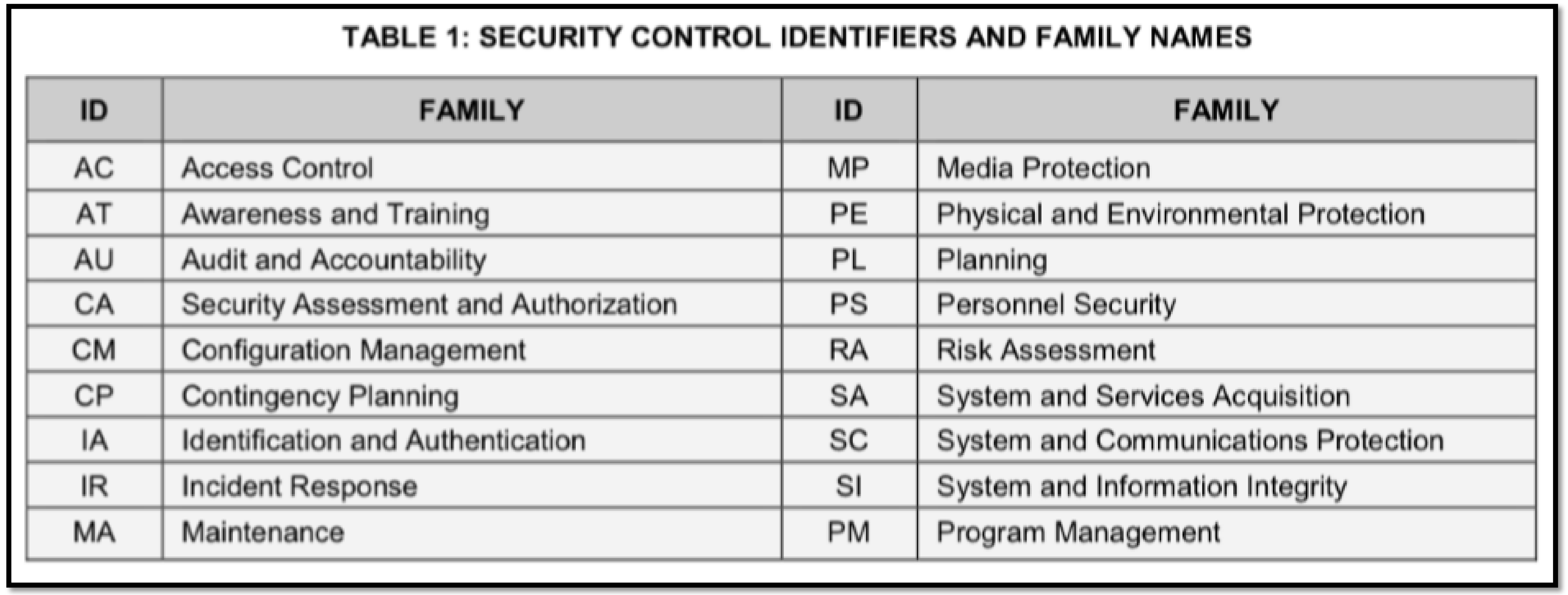
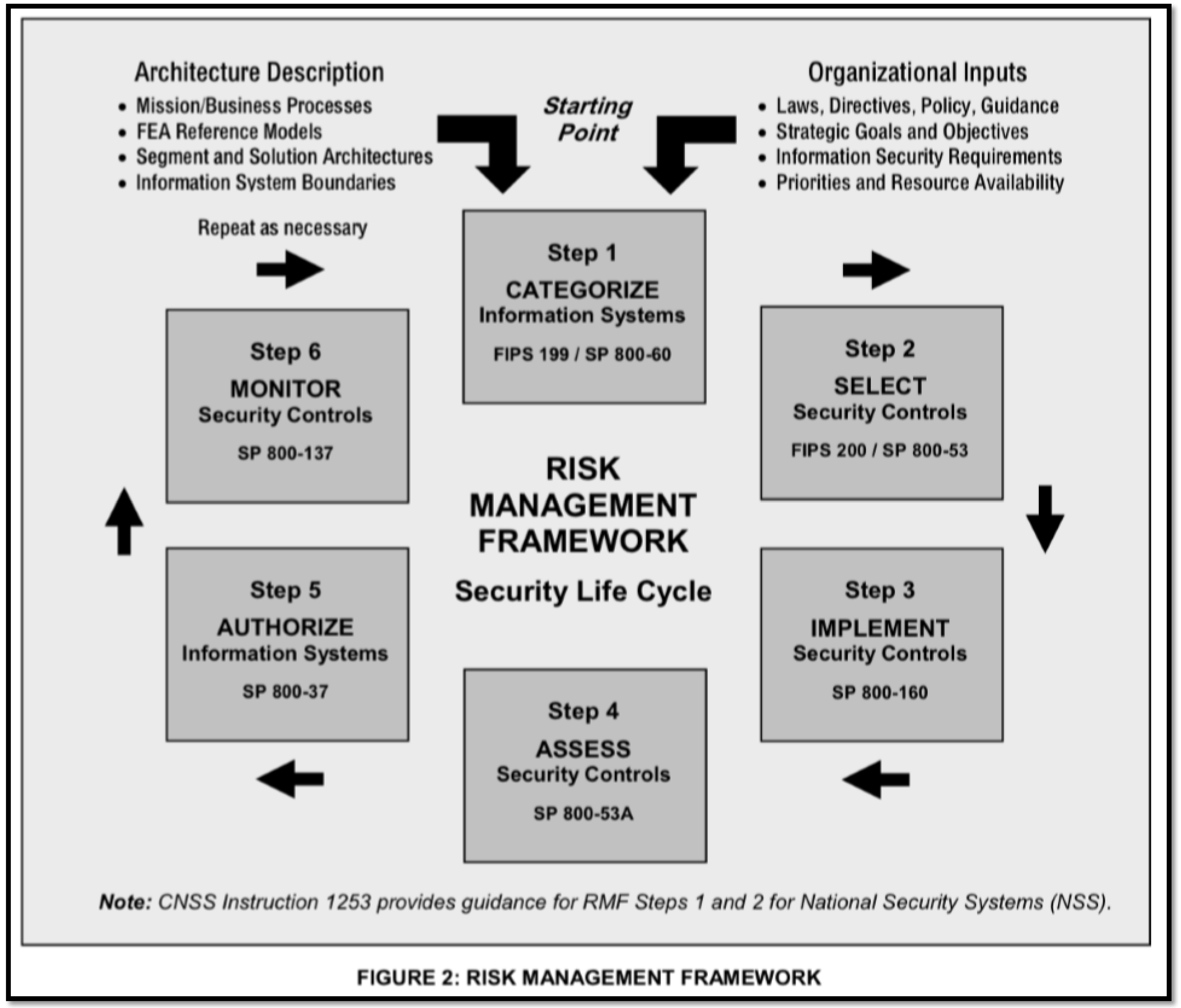


TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

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

Control Families

RMF



Architecture Description

- Mission/Business Processes
- FEA Reference Models
- Segment and Solution Architectures
- Information System Boundaries

Starting Point

Organizational Inputs

- Laws, Directives, Policy, Guidance
- Strategic Goals and Objectives
- Information Security Requirements
- Priorities and Resource Availability

Repeat as necessary

Step 1 CATEGORIZE Information Systems FIPS 199 / SP 800-60

Step 2 SELECT Security Controls FIPS 200 / SP 800-53

Step 3 IMPLEMENT Security Controls SP 800-160

Step 4 ASSESS Security Controls SP 800-53A

Step 5 AUTHORIZE Information Systems SP 800-37

Step 6 MONITOR Security Controls SP 800-137

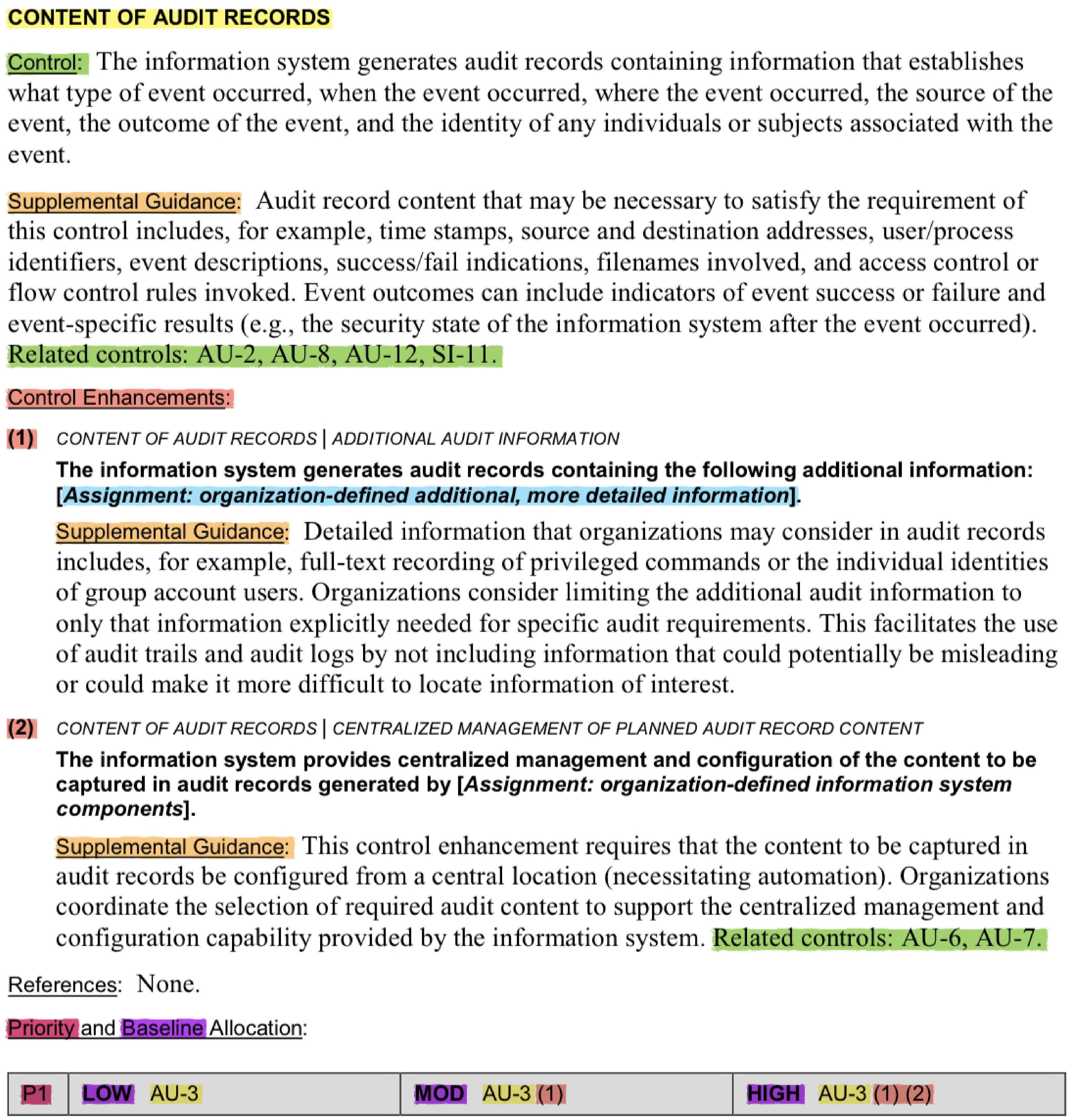
RISK MANAGEMENT FRAMEWORK

Security Life Cycle

Note: *CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).*

FIGURE 2: RISK MANAGEMENT FRAMEWORK

NIST 800-53r4 Annex F: Controls



CONTENT OF AUDIT RECORDS

Control: The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event.

Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the information system after the event occurred). Related controls: AU-2, AU-8, AU-12, SI-11.

Control Enhancements:

(1) *CONTENT OF AUDIT RECORDS | ADDITIONAL AUDIT INFORMATION*

The information system generates audit records containing the following additional information: [*Assignment: organization-defined additional, more detailed information*].

Supplemental Guidance: Detailed information that organizations may consider in audit records includes, for example, full-text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest.

(2) *CONTENT OF AUDIT RECORDS | CENTRALIZED MANAGEMENT OF PLANNED AUDIT RECORD CONTENT*

The information system provides centralized management and configuration of the content to be captured in audit records generated by [*Assignment: organization-defined information system components*].

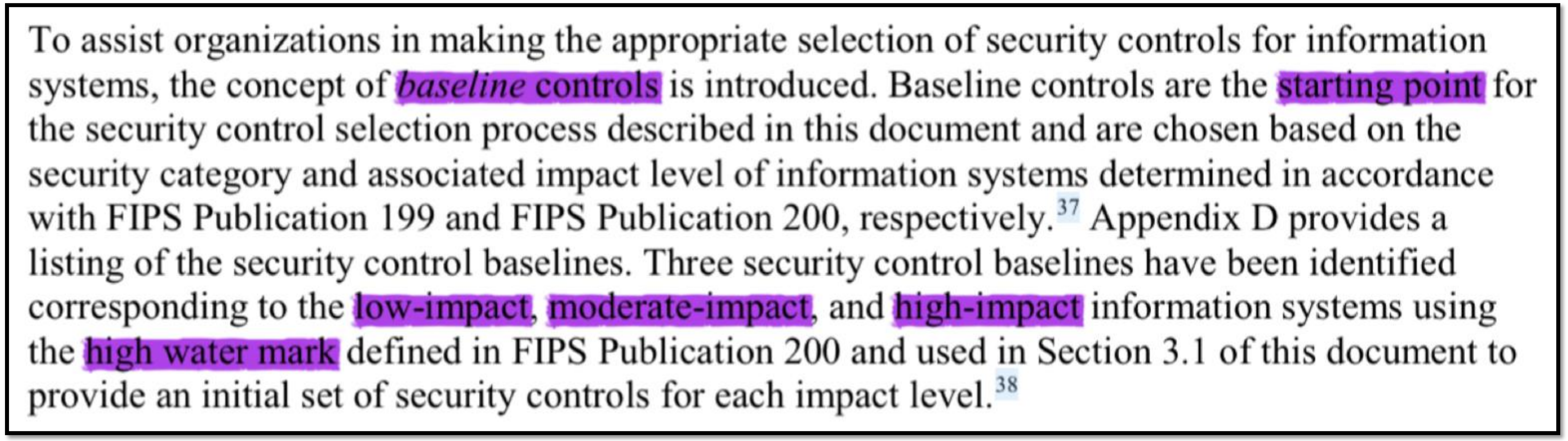
Supplemental Guidance: This control enhancement requires that the content to be captured in audit records be configured from a central location (necessitating automation). Organizations coordinate the selection of required audit content to support the centralized management and configuration capability provided by the information system. Related controls: AU-6, AU-7.

References: None.

Priority and Baseline Allocation:

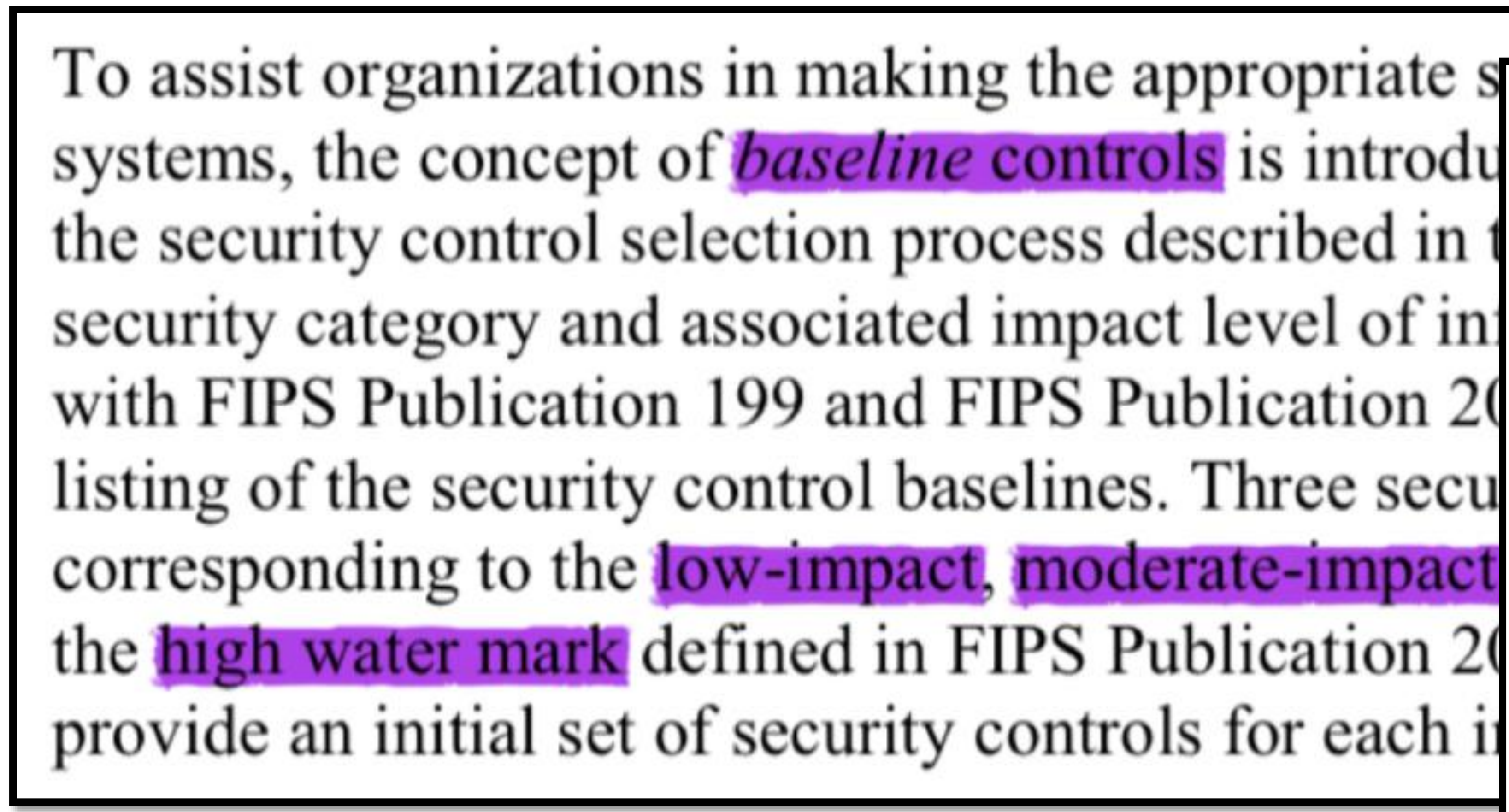
P1	LOW AU-3	MOD AU-3 (1)	HIGH AU-3 (1) (2)

NIST 800-53r4 Baselines



To assist organizations in making the appropriate selection of security controls for information systems, the concept of *baseline* controls is introduced. Baseline controls are the starting point for the security control selection process described in this document and are chosen based on the security category and associated impact level of information systems determined in accordance with FIPS Publication 199 and FIPS Publication 200, respectively.[37] Appendix D provides a listing of the security control baselines. Three security control baselines have been identified corresponding to the low-impact, moderate-impact, and high-impact information systems using the high water mark defined in FIPS Publication 200 and used in Section 3.1 of this document to provide an initial set of security controls for each impact level.[38]

NIST 800-53r4 Baselines



To assist organizations in making the appropriate s
systems, the concept of *baseline controls* is introdu
the security control selection process described in t
security category and associated impact level of in
with FIPS Publication 199 and FIPS Publication 20
listing of the security control baselines. Three secu
corresponding to the low-impact, moderate-impact
the high water mark defined in FIPS Publication 20
provide an initial set of security controls for each i

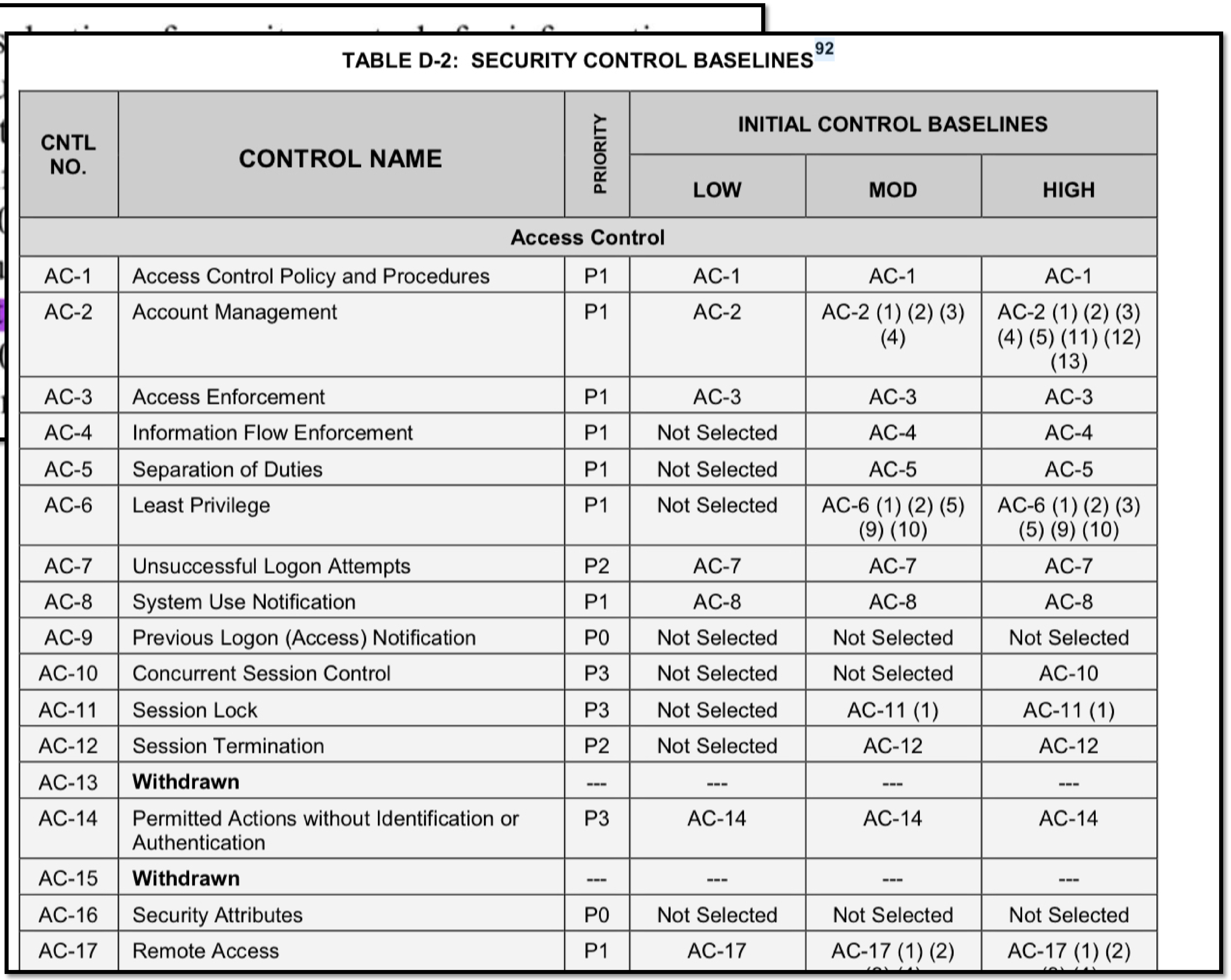
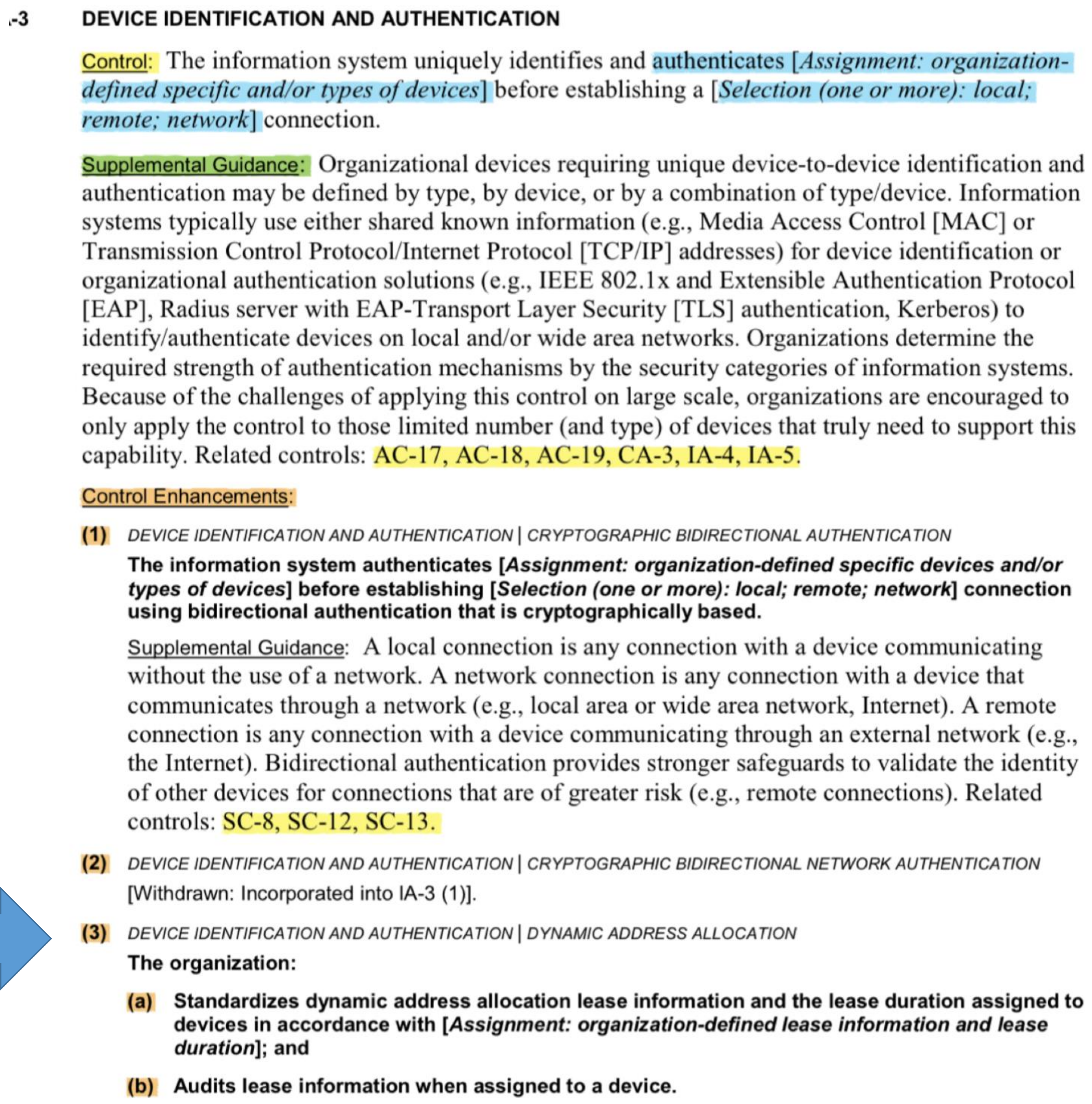


TABLE D-2: SECURITY CONTROL BASELINES[92]

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
	Access Control				
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-2	Account Management	P1	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)
AC-3	Access Enforcement	P1	AC-3	AC-3	AC-3
AC-4	Information Flow Enforcement	P1	Not Selected	AC-4	AC-4
AC-5	Separation of Duties	P1	Not Selected	AC-5	AC-5
AC-6	Least Privilege	P1	Not Selected	AC-6 (1) (2) (5) (9) (10)	AC-6 (1) (2) (3) (5) (9) (10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-8	System Use Notification	P1	AC-8	AC-8	AC-8
AC-9	Previous Logon (Access) Notification	P0	Not Selected	Not Selected	Not Selected
AC-10	Concurrent Session Control	P3	Not Selected	Not Selected	AC-10
AC-11	Session Lock	P3	Not Selected	AC-11 (1)	AC-11 (1)
AC-12	Session Termination	P2	Not Selected	AC-12	AC-12
AC-13	**Withdrawn**	---	---	---	---
AC-14	Permitted Actions without Identification or Authentication	P3	AC-14	AC-14	AC-14
AC-15	**Withdrawn**	---	---	---	---
AC-16	Security Attributes	P0	Not Selected	Not Selected	Not Selected
AC-17	Remote Access	P1	AC-17	AC-17 (1) (2)	AC-17 (1) (2)

NIST 800-53r4: Assessments?



-3 **DEVICE IDENTIFICATION AND AUTHENTICATION**

Control: The information system uniquely identifies and authenticates [*Assignment: organization-defined specific and/or types of devices*] before establishing a [*Selection (one or more): local; remote; network*] connection.

Supplemental Guidance: Organizational devices requiring unique device-to-device identification and authentication may be defined by type, by device, or by a combination of type/device. Information systems typically use either shared known information (e.g., Media Access Control [MAC] or Transmission Control Protocol/Internet Protocol [TCP/IP] addresses) for device identification or organizational authentication solutions (e.g., IEEE 802.1x and Extensible Authentication Protocol [EAP], Radius server with EAP-Transport Layer Security [TLS] authentication, Kerberos) to identify/authenticate devices on local and/or wide area networks. Organizations determine the required strength of authentication mechanisms by the security categories of information systems. Because of the challenges of applying this control on large scale, organizations are encouraged to only apply the control to those limited number (and type) of devices that truly need to support this capability. Related controls: AC-17, AC-18, AC-19, CA-3, IA-4, IA-5.

Control Enhancements:

(1) *DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION*

The information system authenticates [*Assignment: organization-defined specific devices and/or types of devices*] before establishing [*Selection (one or more): local; remote; network*] connection using bidirectional authentication that is cryptographically based.

Supplemental Guidance: A local connection is any connection with a device communicating without the use of a network. A network connection is any connection with a device that communicates through a network (e.g., local area or wide area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Bidirectional authentication provides stronger safeguards to validate the identity of other devices for connections that are of greater risk (e.g., remote connections). Related controls: SC-8, SC-12, SC-13.

(2) *DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL NETWORK AUTHENTICATION*

[Withdrawn: Incorporated into IA-3 (1)].

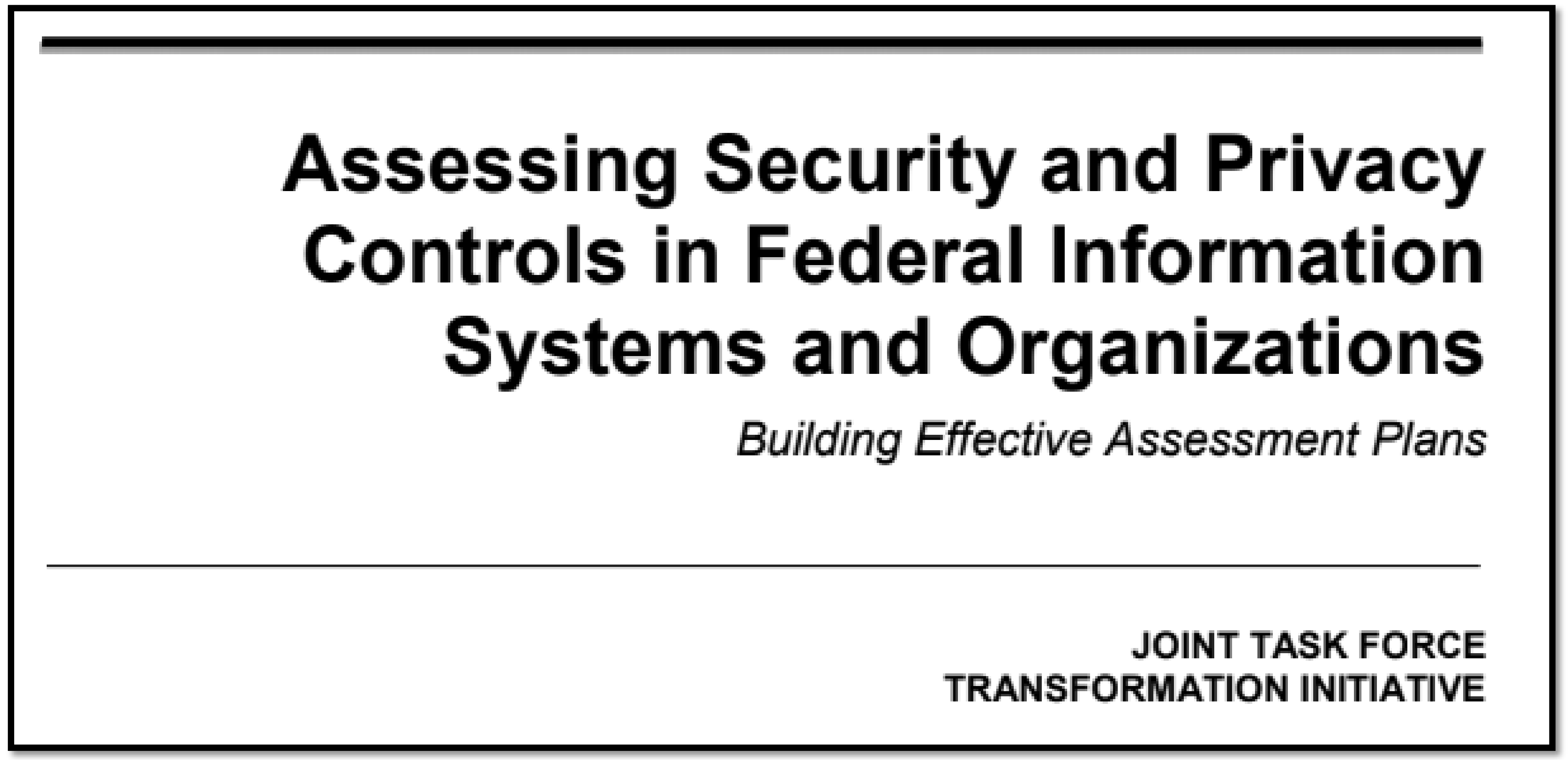
(3) *DEVICE IDENTIFICATION AND AUTHENTICATION | DYNAMIC ADDRESS ALLOCATION*

The organization:

(a) **Standardizes dynamic address allocation lease information and the lease duration assigned to devices in accordance with [*Assignment: organization-defined lease information and lease duration*]; and**

(b) **Audits lease information when assigned to a device.**

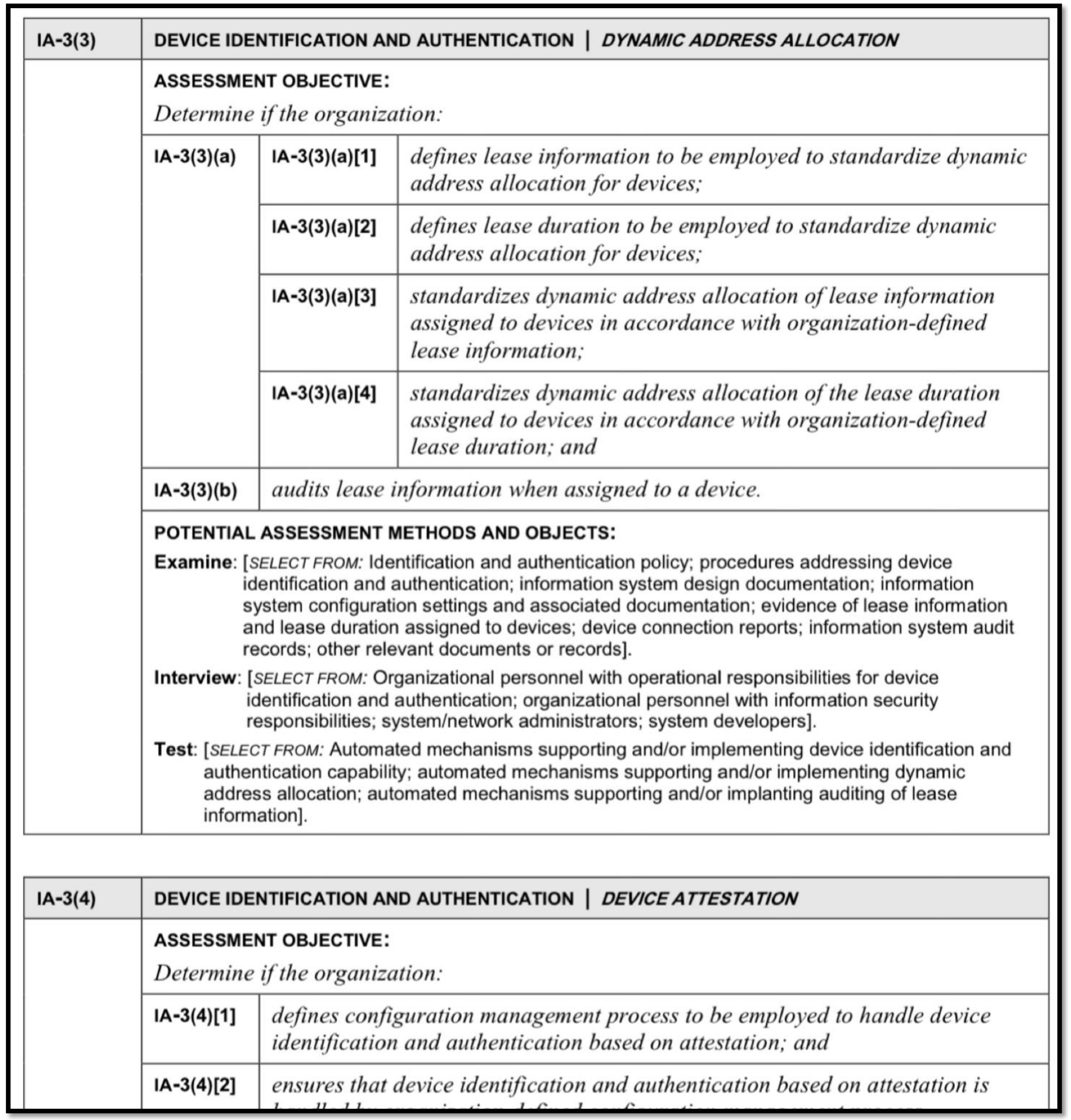
NIST 800-53r4a: Assessments



Assessing Security and Privacy Controls in Federal Information Systems and Organizations

Building Effective Assessment Plans

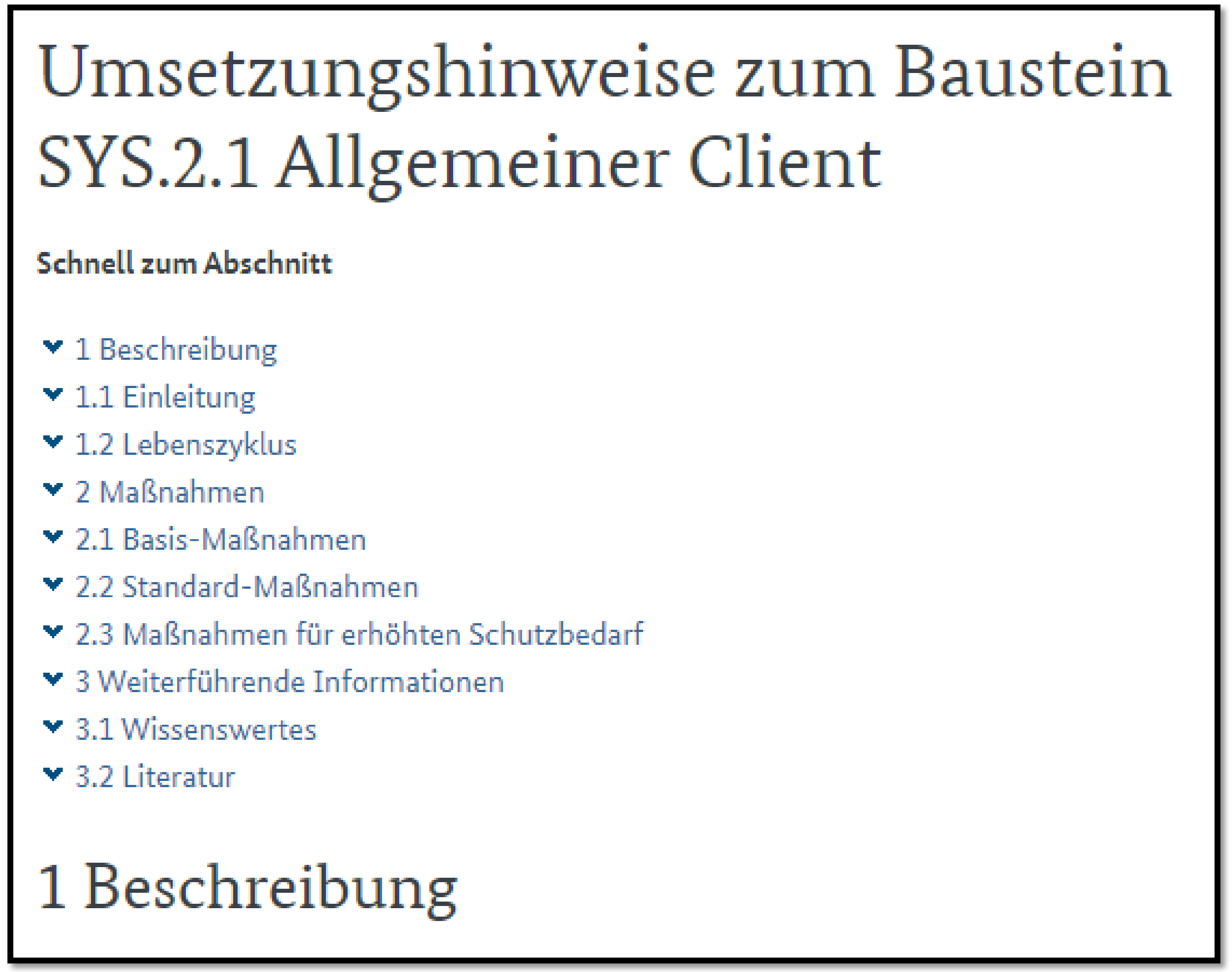
JOINT TASK FORCE
TRANSFORMATION INITIATIVE



IA-3(3)	DEVICE IDENTIFICATION AND AUTHENTICATION | *DYNAMIC ADDRESS ALLOCATION*		
	ASSESSMENT OBJECTIVE: *Determine if the organization:*		
	IA-3(3)(a)	IA-3(3)(a)[1]	*defines lease information to be employed to standardize dynamic address allocation for devices;*
		IA-3(3)(a)[2]	*defines lease duration to be employed to standardize dynamic address allocation for devices;*
		IA-3(3)(a)[3]	*standardizes dynamic address allocation of lease information assigned to devices in accordance with organization-defined lease information;*
		IA-3(3)(a)[4]	*standardizes dynamic address allocation of the lease duration assigned to devices in accordance with organization-defined lease duration; and*
	IA-3(3)(b)	*audits lease information when assigned to a device.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Identification and authentication policy; procedures addressing device identification and authentication; information system design documentation; information system configuration settings and associated documentation; evidence of lease information and lease duration assigned to devices; device connection reports; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* Organizational personnel with operational responsibilities for device identification and authentication; organizational personnel with information security responsibilities; system/network administrators; system developers]. **Test**: [*SELECT FROM:* Automated mechanisms supporting and/or implementing device identification and authentication capability; automated mechanisms supporting and/or implementing dynamic address allocation; automated mechanisms supporting and/or implanting auditing of lease information].		

IA-3(4)	DEVICE IDENTIFICATION AND AUTHENTICATION | *DEVICE ATTESTATION*	
	ASSESSMENT OBJECTIVE: *Determine if the organization:*	
	IA-3(4)[1]	*defines configuration management process to be employed to handle device identification and authentication based on attestation; and*
	IA-3(4)[2]	*ensures that device identification and authentication based on attestation is*

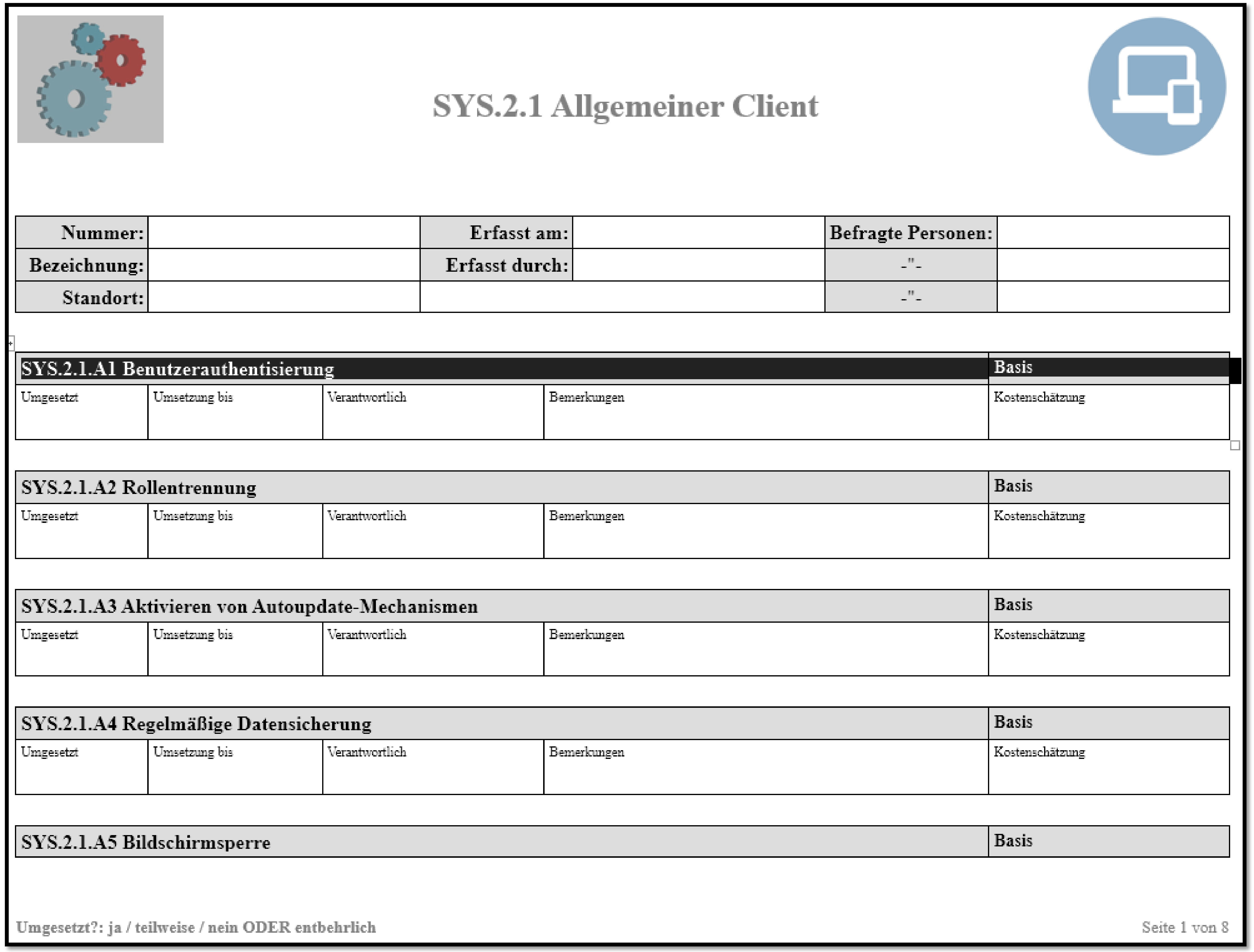
Vgl.: IT-Grundschutz-Kompendium Checklisten



Umsetzungshinweise zum Baustein SYS.2.1 Allgemeiner Client

Schnell zum Abschnitt

1 Beschreibung



SYS.2.1 Allgemeiner Client

Nummer:		Erfasst am:		Befragte Personen:	
Bezeichnung:		Erfasst durch:		-"-	
Standort:				-"-	

SYS.2.1.A1 Benutzerauthentisierung				Basis
Umgesetzt	Umsetzung bis	Verantwortlich	Bemerkungen	Kostenschätzung

SYS.2.1.A2 Rollentrennung				Basis
Umgesetzt	Umsetzung bis	Verantwortlich	Bemerkungen	Kostenschätzung

SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen				Basis
Umgesetzt	Umsetzung bis	Verantwortlich	Bemerkungen	Kostenschätzung

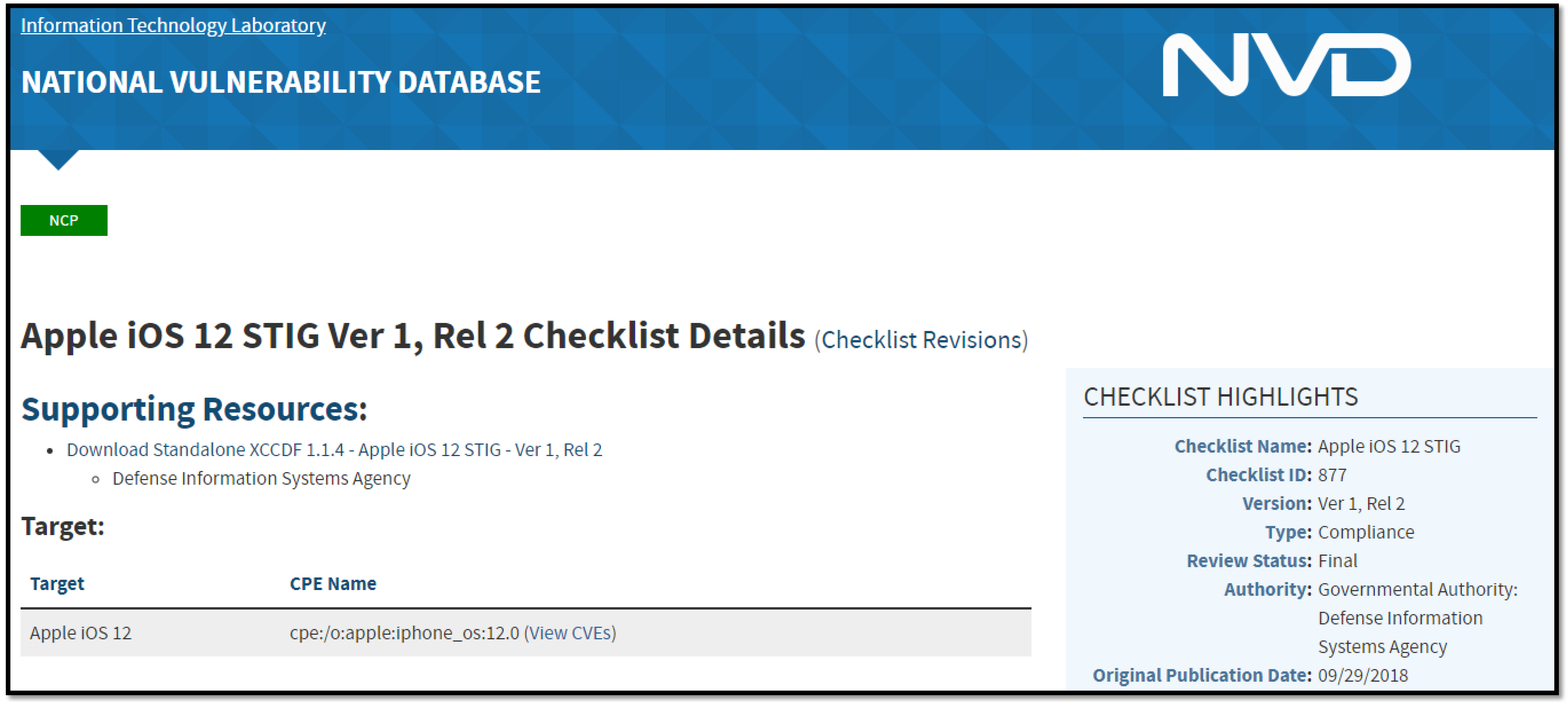
SYS.2.1.A4 Regelmäßige Datensicherung				Basis
Umgesetzt	Umsetzung bis	Verantwortlich	Bemerkungen	Kostenschätzung

SYS.2.1.A5 Bildschirmsperre				Basis

Umgesetzt?: ja / teilweise / nein ODER entbehrlich

Seite 1 von 8

DISA STIGs



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

Apple iOS 12 STIG Ver 1, Rel 2 Checklist Details (Checklist Revisions)

Supporting Resources:

- Download Standalone XCCDF 1.1.4 - Apple iOS 12 STIG - Ver 1, Rel 2
  - Defense Information Systems Agency

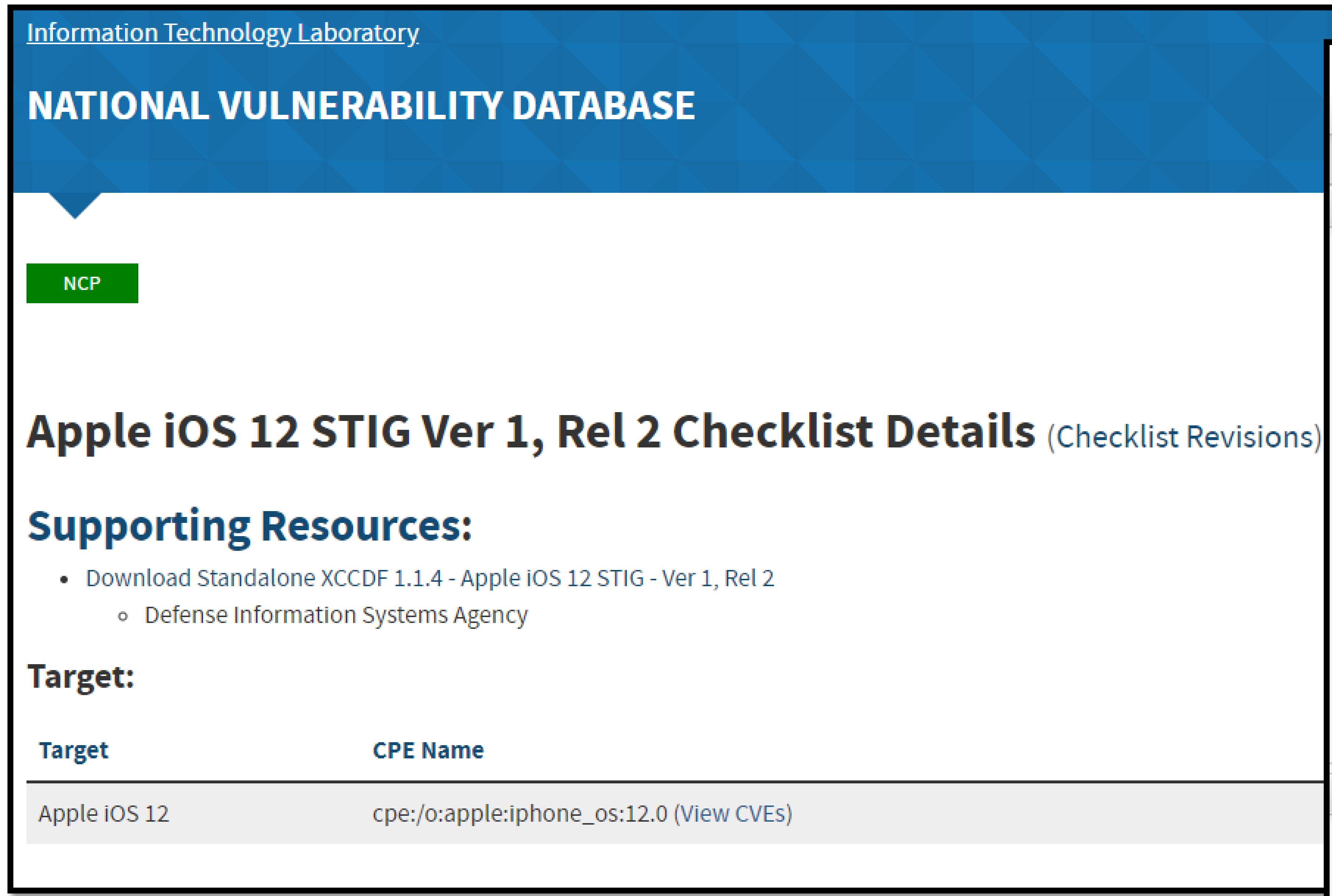
Target:

Target	CPE Name
Apple iOS 12	cpe:/o:apple:iphone_os:12.0 (View CVEs)

CHECKLIST HIGHLIGHTS

Checklist Name: Apple iOS 12 STIG
Checklist ID: 877
Version: Ver 1, Rel 2
Type: Compliance
Review Status: Final
Authority: Governmental Authority: Defense Information Systems Agency
Original Publication Date: 09/29/2018

DISA STIGs



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

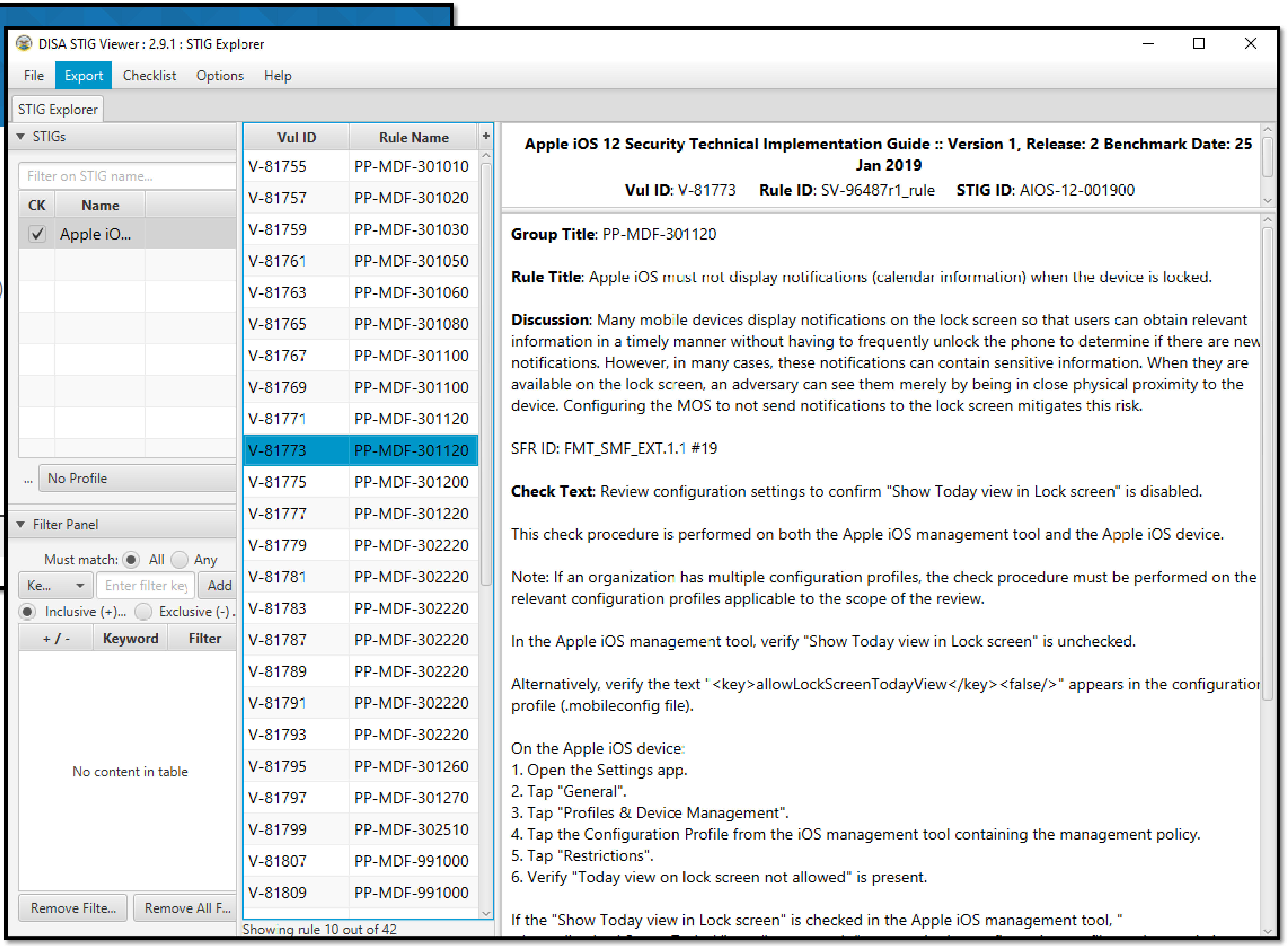
Apple iOS 12 STIG Ver 1, Rel 2 Checklist Details (Checklist Revisions)

Supporting Resources:

- Download Standalone XCCDF 1.1.4 - Apple iOS 12 STIG - Ver 1, Rel 2
  - Defense Information Systems Agency

Target:

Target	CPE Name
Apple iOS 12	cpe:/o:apple:iphone_os:12.0 (View CVEs)



CK	Name
☑	Apple iO...

Must match: ● All ○ Any

● Inclusive (+)... ○ Exclusive (-)...

Vul ID	Rule Name
V-81755	PP-MDF-301010
V-81757	PP-MDF-301020
V-81759	PP-MDF-301030
V-81761	PP-MDF-301050
V-81763	PP-MDF-301060
V-81765	PP-MDF-301080
V-81767	PP-MDF-301100
V-81769	PP-MDF-301100
V-81771	PP-MDF-301120
V-81773	PP-MDF-301120
V-81775	PP-MDF-301200
V-81777	PP-MDF-301220
V-81779	PP-MDF-302220
V-81781	PP-MDF-302220
V-81783	PP-MDF-302220
V-81787	PP-MDF-302220
V-81789	PP-MDF-302220
V-81791	PP-MDF-302220
V-81793	PP-MDF-302220
V-81795	PP-MDF-301260
V-81797	PP-MDF-301270
V-81799	PP-MDF-302510
V-81807	PP-MDF-991000
V-81809	PP-MDF-991000

Showing rule 10 out of 42

Apple iOS 12 Security Technical Implementation Guide :: Version 1, Release: 2 Benchmark Date: 25 Jan 2019

Vul ID: V-81773 **Rule ID**: SV-96487r1_rule **STIG ID**: AIOS-12-001900

Group Title: PP-MDF-301120

Rule Title: Apple iOS must not display notifications (calendar information) when the device is locked.

Discussion: Many mobile devices display notifications on the lock screen so that users can obtain relevant information in a timely manner without having to frequently unlock the phone to determine if there are new notifications. However, in many cases, these notifications can contain sensitive information. When they are available on the lock screen, an adversary can see them merely by being in close physical proximity to the device. Configuring the MOS to not send notifications to the lock screen mitigates this risk.

SFR ID: FMT_SMF_EXT.1.1 #19

Check Text: Review configuration settings to confirm "Show Today view in Lock screen" is disabled.

This check procedure is performed on both the Apple iOS management tool and the Apple iOS device.

Note: If an organization has multiple configuration profiles, the check procedure must be performed on the relevant configuration profiles applicable to the scope of the review.

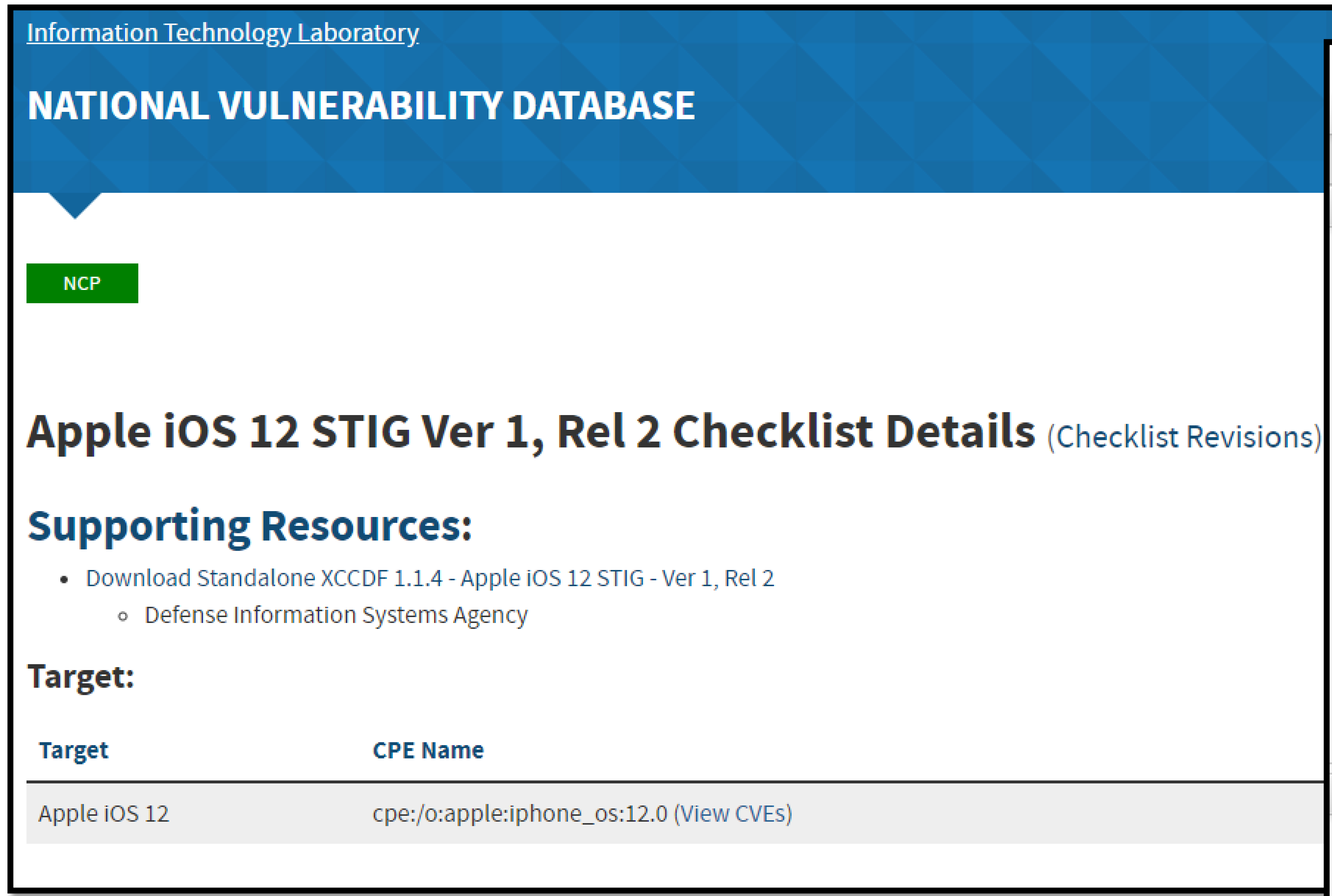
In the Apple iOS management tool, verify "Show Today view in Lock screen" is unchecked.

Alternatively, verify the text "<key>allowLockScreenTodayView</key><false/>" appears in the configuration profile (.mobileconfig file).

On the Apple iOS device:
1. Open the Settings app.
2. Tap "General".
3. Tap "Profiles & Device Management".
4. Tap the Configuration Profile from the iOS management tool containing the management policy.
5. Tap "Restrictions".
6. Verify "Today view on lock screen not allowed" is present.

If the "Show Today view in Lock screen" is checked in the Apple iOS management tool, "

DISA STIGs



Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NCP

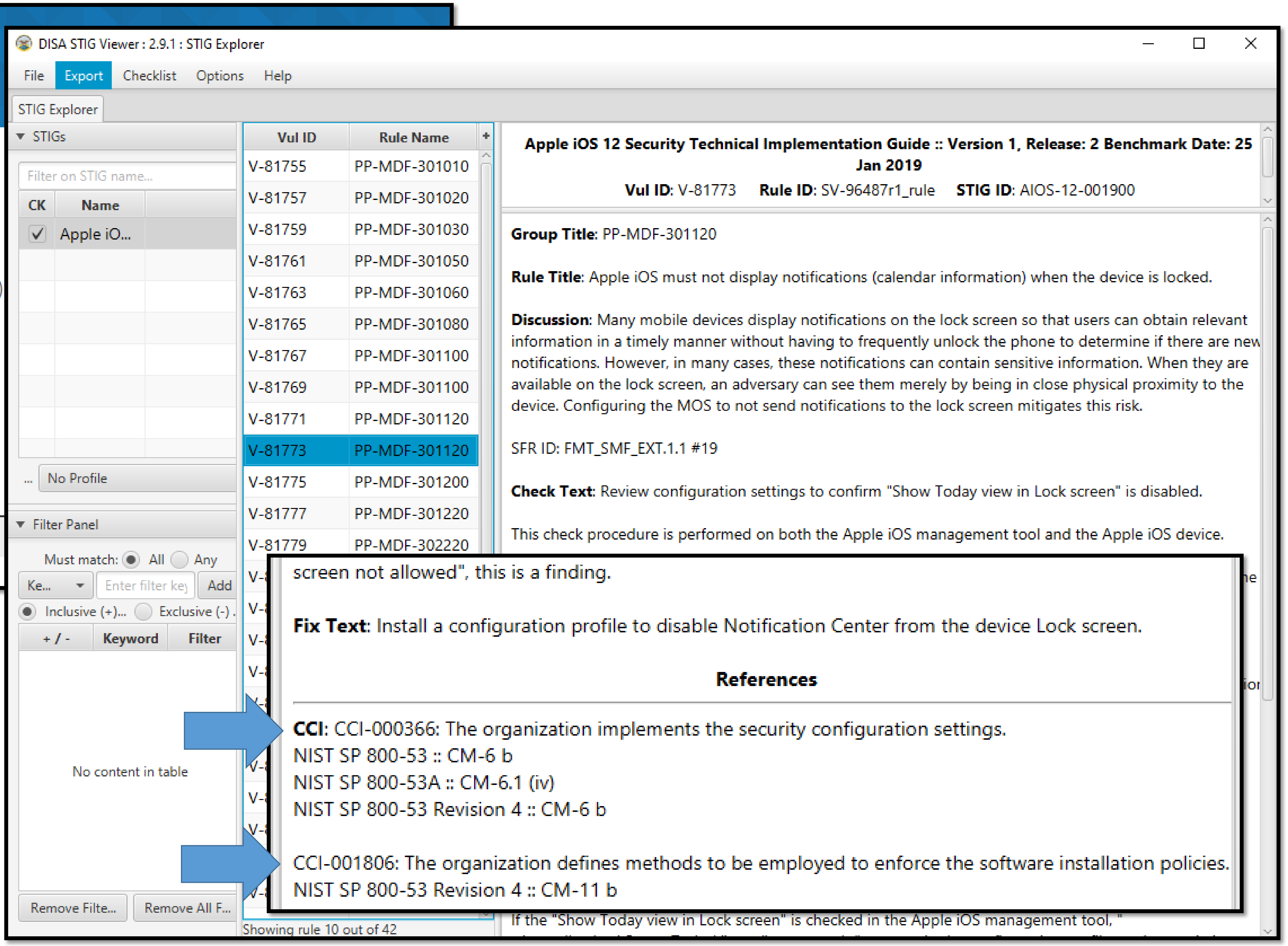
Apple iOS 12 STIG Ver 1, Rel 2 Checklist Details (Checklist Revisions)

Supporting Resources:

- Download Standalone XCCDF 1.1.4 - Apple iOS 12 STIG - Ver 1, Rel 2
  - Defense Information Systems Agency

Target:

Target	CPE Name
Apple iOS 12	cpe:/o:apple:iphone_os:12.0 (View CVEs)



Vul ID	Rule Name
V-81755	PP-MDF-301010
V-81757	PP-MDF-301020
V-81759	PP-MDF-301030
V-81761	PP-MDF-301050
V-81763	PP-MDF-301060
V-81765	PP-MDF-301080
V-81767	PP-MDF-301100
V-81769	PP-MDF-301100
V-81771	PP-MDF-301120
V-81773	PP-MDF-301120
V-81775	PP-MDF-301200
V-81777	PP-MDF-301220
V-81779	PP-MDF-302220

Showing rule 10 out of 42

Apple iOS 12 Security Technical Implementation Guide :: Version 1, Release: 2 Benchmark Date: 25 Jan 2019

Vul ID: V-81773 **Rule ID**: SV-96487r1_rule **STIG ID**: AIOS-12-001900

Group Title: PP-MDF-301120

Rule Title: Apple iOS must not display notifications (calendar information) when the device is locked.

Discussion: Many mobile devices display notifications on the lock screen so that users can obtain relevant information in a timely manner without having to frequently unlock the phone to determine if there are new notifications. However, in many cases, these notifications can contain sensitive information. When they are available on the lock screen, an adversary can see them merely by being in close physical proximity to the device. Configuring the MOS to not send notifications to the lock screen mitigates this risk.

SFR ID: FMT_SMF_EXT.1.1 #19

Check Text: Review configuration settings to confirm "Show Today view in Lock screen" is disabled.

This check procedure is performed on both the Apple iOS management tool and the Apple iOS device.

screen not allowed", this is a finding.

Fix Text: Install a configuration profile to disable Notification Center from the device Lock screen.

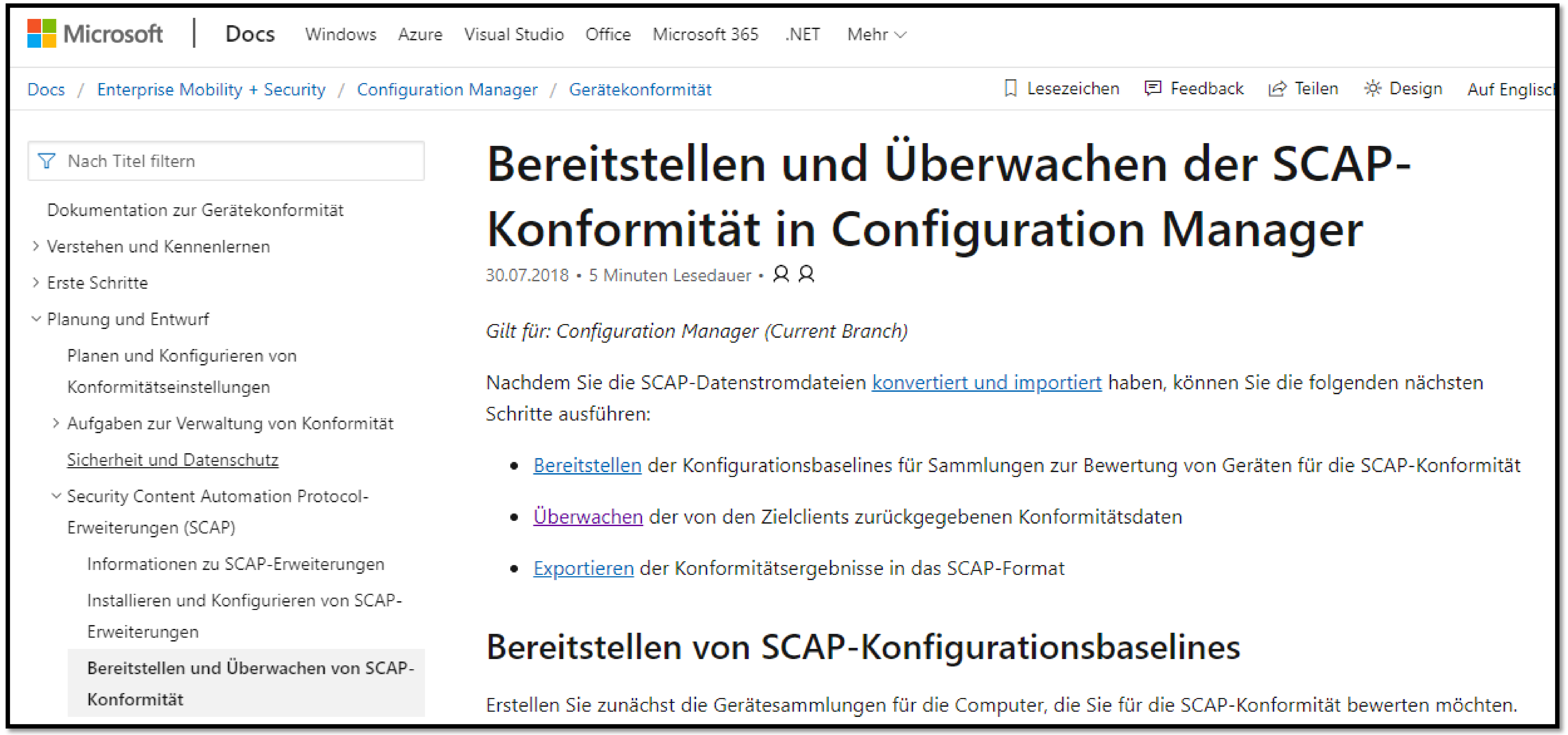
References

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

CCI-001806: The organization defines methods to be employed to enforce the software installation policies.
NIST SP 800-53 Revision 4 :: CM-11 b

If the "Show Today view in Lock screen" is checked in the Apple iOS management tool, "

SCAP OVAL



Microsoft | Docs Windows Azure Visual Studio Office Microsoft 365 .NET Mehr
Docs / Enterprise Mobility + Security / Configuration Manager / Gerätekonformität
Lesezeichen Feedback Teilen Design Auf Englisc
Nach Titel filtern
Dokumentation zur Gerätekonformität
Verstehen und Kennenlernen
Erste Schritte
Planung und Entwurf
Planen und Konfigurieren von Konformitätseinstellungen
Aufgaben zur Verwaltung von Konformität
Sicherheit und Datenschutz
Security Content Automation Protocol-Erweiterungen (SCAP)
Informationen zu SCAP-Erweiterungen
Installieren und Konfigurieren von SCAP-Erweiterungen
Bereitstellen und Überwachen von SCAP-Konformität

Bereitstellen und Überwachen der SCAP-Konformität in Configuration Manager

30.07.2018 • 5 Minuten Lesedauer •

Gilt für: Configuration Manager (Current Branch)

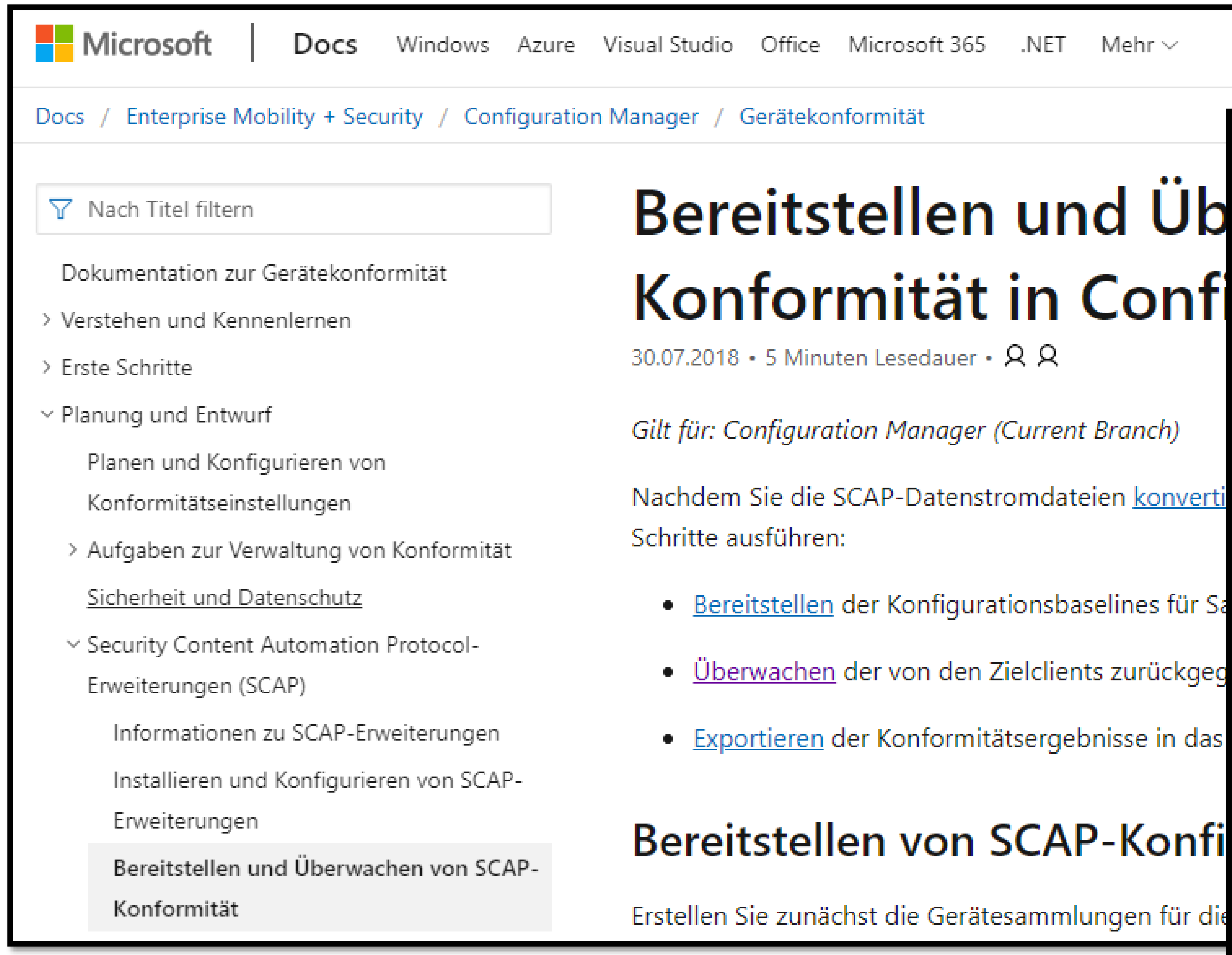
Nachdem Sie die SCAP-Datenstromdateien konvertiert und importiert haben, können Sie die folgenden nächsten Schritte ausführen:

- Bereitstellen der Konfigurationsbaselines für Sammlungen zur Bewertung von Geräten für die SCAP-Konformität
- Überwachen der von den Zielclients zurückgegebenen Konformitätsdaten
- Exportieren der Konformitätsergebnisse in das SCAP-Format

Bereitstellen von SCAP-Konfigurationsbaselines

Erstellen Sie zunächst die Gerätesammlungen für die Computer, die Sie für die SCAP-Konformität bewerten möchten.

SCAP OVAL



Microsoft | Docs Windows Azure Visual Studio Office Microsoft 365 .NET Mehr

Docs / Enterprise Mobility + Security / Configuration Manager / Gerätekonformität

Nach Titel filtern

- Dokumentation zur Gerätekonformität
- Verstehen und Kennenlernen
- Erste Schritte
- Planung und Entwurf
  - Planen und Konfigurieren von Konformitätseinstellungen
  - Aufgaben zur Verwaltung von Konformität
  - Sicherheit und Datenschutz
  - Security Content Automation Protocol-Erweiterungen (SCAP)
    - Informationen zu SCAP-Erweiterungen
    - Installieren und Konfigurieren von SCAP-Erweiterungen
    - Bereitstellen und Überwachen von SCAP-Konformität

Bereitstellen und Üb Konformität in Confi

30.07.2018 • 5 Minuten Lesedauer •

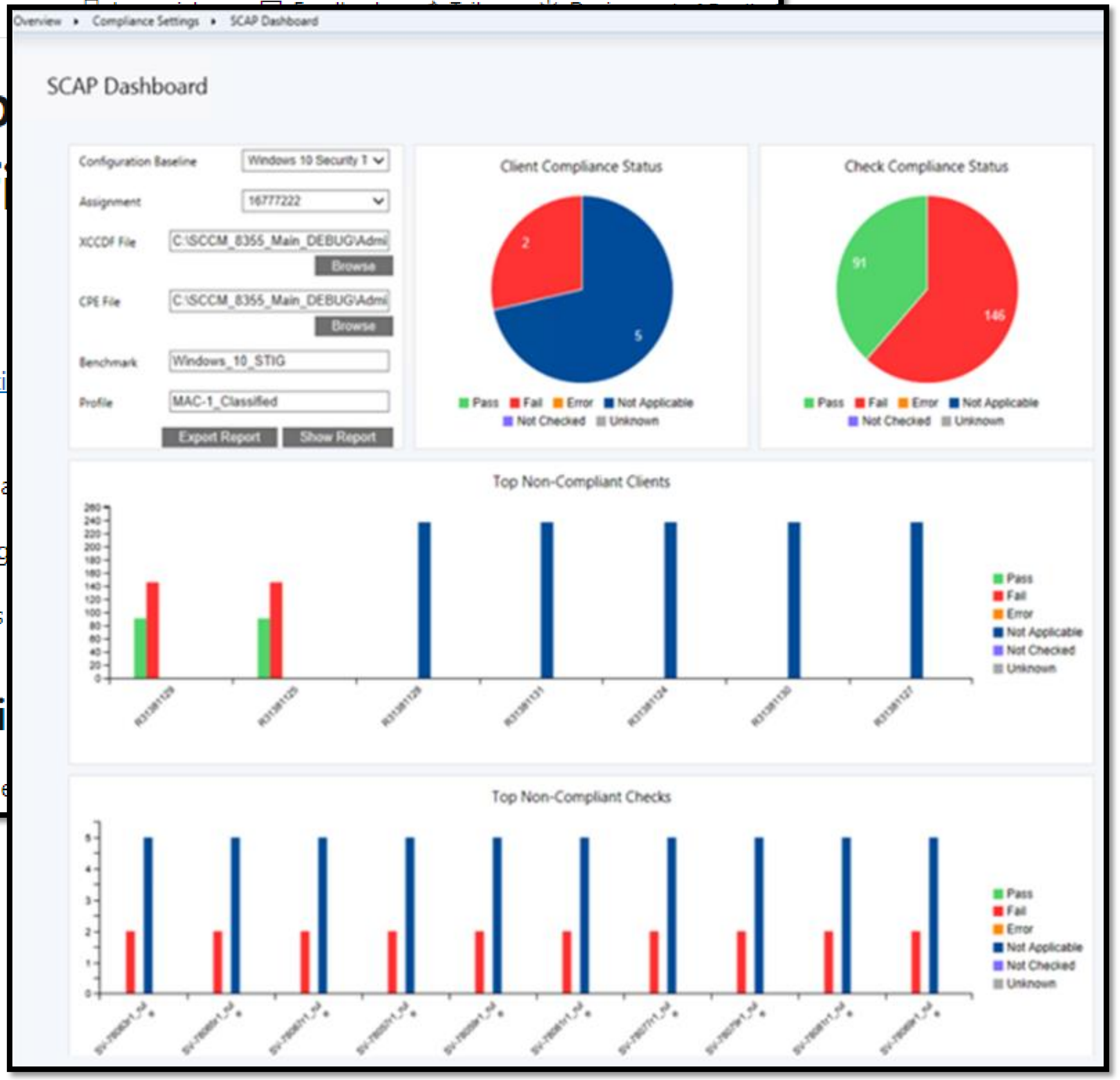
Gilt für: Configuration Manager (Current Branch)

Nachdem Sie die SCAP-Datenstromdateien konverti Schritte ausführen:

- Bereitstellen der Konfigurationsbaselines für Sa
- Überwachen der von den Zielclients zurückgeg
- Exportieren der Konformitätsergebnisse in das

Bereitstellen von SCAP-Konfi

Erstellen Sie zunächst die Gerätesammlungen für die



Overview ▸ Compliance Settings ▸ SCAP Dashboard

SCAP Dashboard

Configuration Baseline: Windows 10 Security 1

Assignment: 16777222

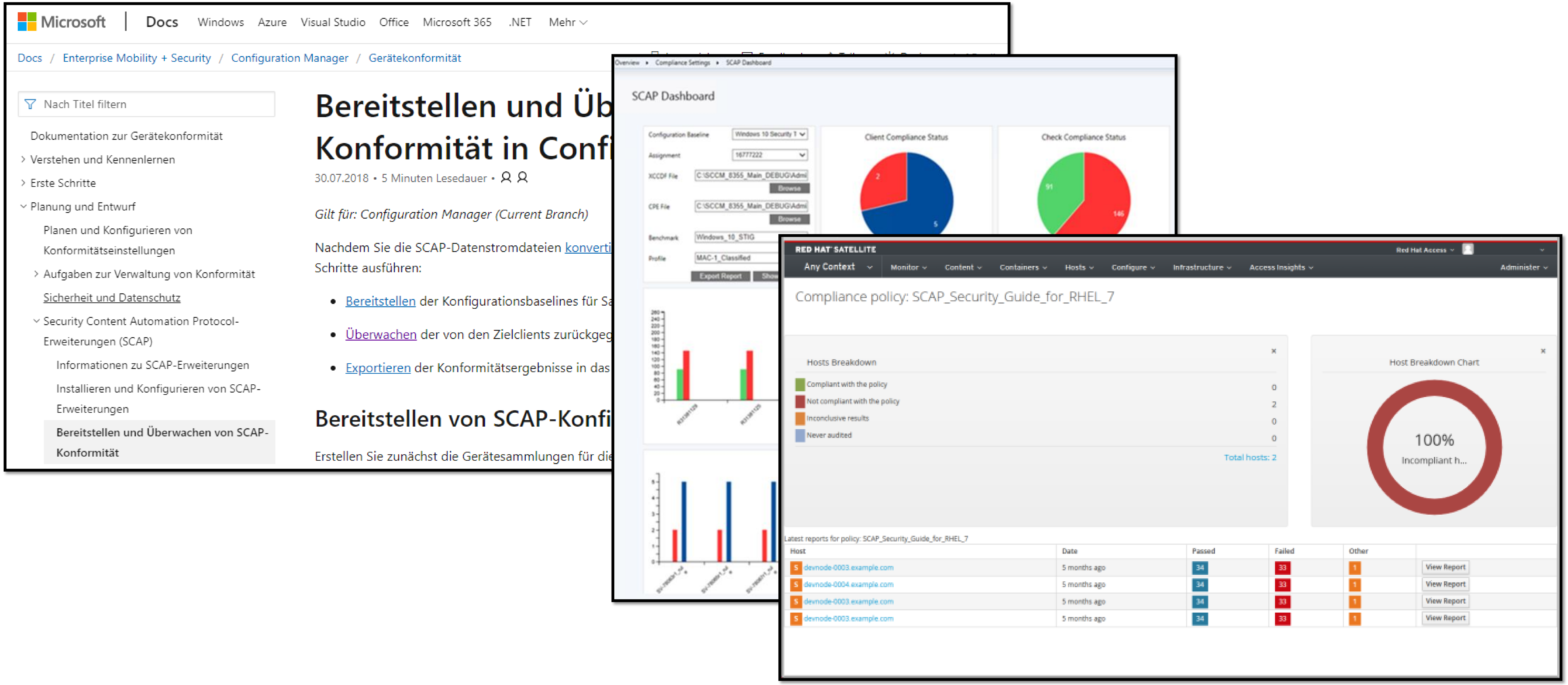
XCCDF File: C:\SCCM_8355_Main_DEBUG\Admi

CPE File: C:\SCCM_8355_Main_DEBUG\Admi

Benchmark: Windows_10_STIG

Profile: MAC-1_Classified

SCAP OVAL



Docs / Enterprise Mobility + Security / Configuration Manager / Gerätekonformität

Dokumentation zur Gerätekonformität

Verstehen und Kennenlernen

Erste Schritte

Planung und Entwurf

Planen und Konfigurieren von Konformitätseinstellungen

Aufgaben zur Verwaltung von Konformität

Sicherheit und Datenschutz

Security Content Automation Protocol-Erweiterungen (SCAP)

Informationen zu SCAP-Erweiterungen

Installieren und Konfigurieren von SCAP-Erweiterungen

Bereitstellen und Überwachen von SCAP-Konformität

Bereitstellen und Üb
Konformität in Confi

30.07.2018 • 5 Minuten Lesedauer •

Gilt für: Configuration Manager (Current Branch)

Nachdem Sie die SCAP-Datenstromdateien konverti
Schritte ausführen:

- Bereitstellen der Konfigurationsbaselines für Sa
- Überwachen der von den Zielclients zurückgeg
- Exportieren der Konformitätsergebnisse in das

Bereitstellen von SCAP-Konfi

Erstellen Sie zunächst die Gerätesammlungen für die

Overview ▸ Compliance Settings ▸ SCAP Dashboard

SCAP Dashboard

Configuration Baseline	Windows 10 Security 1
Assignment	16777222
XCCDF File	C:\SCCM_8355_Main_DEBUG\Admi
CPE File	C:\SCCM_8355_Main_DEBUG\Admi
Benchmark	Windows_10_STIG
Profile	MAC-1_Classified

Client Compliance Status

Check Compliance Status

RED HAT SATELLITE

Compliance policy: SCAP_Security_Guide_for_RHEL_7

Hosts Breakdown

🟩 Compliant with the policy	0
🟥 Not compliant with the policy	2
🟧 Inconclusive results	0
🟦 Never audited	0

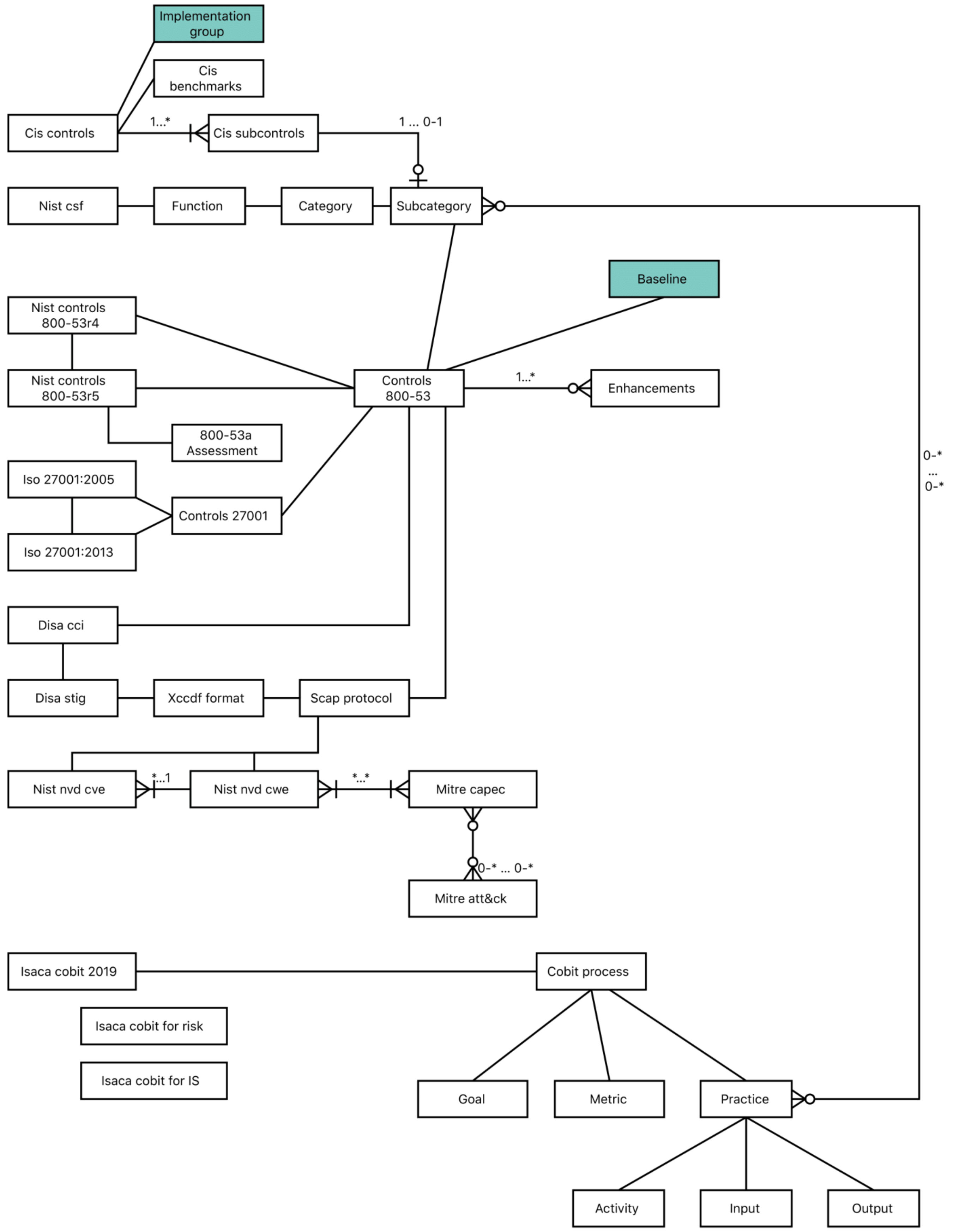
Total hosts: 2

Host Breakdown Chart

Latest reports for policy: SCAP_Security_Guide_for_RHEL_7

Host	Date	Passed	Failed	Other	
S devnode-0003.example.com	5 months ago	34	33	1	View Report
S devnode-0004.example.com	5 months ago	34	33	1	View Report
S devnode-0003.example.com	5 months ago	34	33	1	View Report
S devnode-0003.example.com	5 months ago	34	33	1	View Report

Standard-Korrelationen



Implementation group
Cis benchmarks
Cis controls
1...*
Cis subcontrols
1 ... 0-1
Nist csf
Function
Category
Subcategory
Baseline
Nist controls 800-53r4
Nist controls 800-53r5
Controls 800-53
1...*
Enhancements
800-53a Assessment
0-* ... 0-*
Iso 27001:2005
Controls 27001
Iso 27001:2013
Disa cci
Disa stig
Xccdf format
Scap protocol
Nist nvd cve
*...1
Nist nvd cwe
...
Mitre capec
0-* ... 0-*
Mitre att&ck
Isaca cobit 2019
Cobit process
Isaca cobit for risk
Isaca cobit for IS
Goal
Metric
Practice
Activity
Input
Output