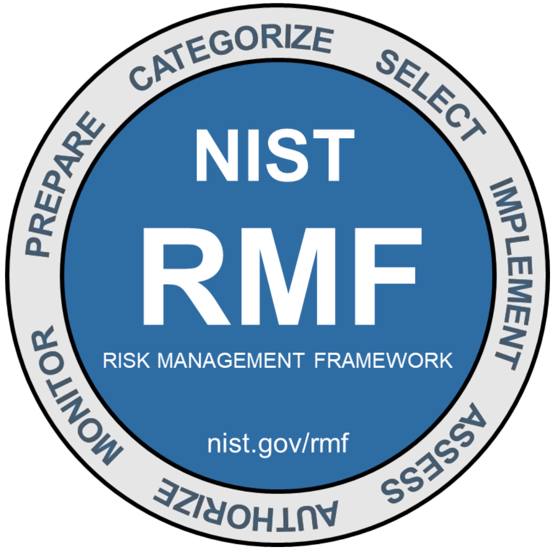
What’s New in SP 800-53A Revision 5

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

Jessica Dickson
jessica.dickson@nist.gov

Victoria Yan Pillitteri
victoria.yan@nist.gov

Overview: NIST SP 800-53A Revision 5



- **Each 800-53 publication provides guidance for implementing specific steps in the RMF.**
  - SP 800-53 and SP 800-53B: address the **Select** step of the RMF and provide guidance on security and privacy control selection (i.e., determining the controls needed to manage risks to organizational operations and assets, individuals, other organizations, and the Nation).
  - SP 800-53A addresses the **Assess** and **Monitor** steps of the RMF and provides guidance on the security and privacy control assessment processes.

Overview: NIST SP 800-53A Revision 5

Purpose: To facilitate (SP 800-53) control assessments within an effective risk management framework

1. Process to conduct effective control assessments (Prepare, Develop Plans, Conduct Assessments, Analyze Results)
2. (Initial) assessment procedures that correspond with SP 800-53 Rev 5 controls

SP 800-53 control assessments:

- ☑ Determine overall effectiveness of implemented controls
- ☑ Indication of quality of risk management process
- ☑ Information about security & privacy strengths/weaknesses of the system/organization

- 🚫 Checklist for compliance
- 🚫 Simple pass/fail results
- 🚫 Paperwork exercise to pass inspections/audits

What’s new in NIST SP 800-53A Revision 5

NIST SP 800-53A, Revision 5 includes:

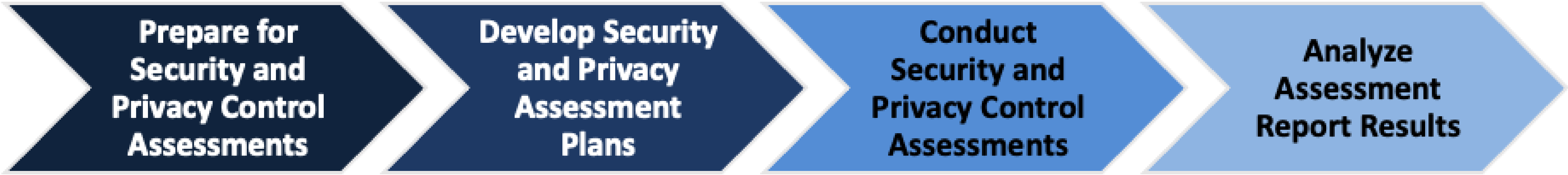
- Updated guidance on the **process to assess controls effectively** (front matter)
- **Updated assessment procedures** to correspond with SP 800-53, Rev 5 controls
    - First-ever procedures for privacy controls
- **New assessment procedure structure** to:
    - Provide better traceability between assessment procedures & controls
    - Improve the efficiency of conducting control assessments
    - Better support the use of automated tools, continuous monitoring, and ongoing authorization programs
- **Assessment procedures in multiple data formats:** CSV, plain text, and OSCAL (XML, YAML, JSON)

NIST SPECIAL PUBLICATION
SP 800-53A
53A
REVISION 5
ASSESSING
SECURITY AND PRIVACY CONTROLS
IN INFORMATION SYSTEMS
AND ORGANIZATIONS
RISK MANAGEMENT FRAMEWORK

NIST SP 800-53A, Revision 5
Published January 25, 2022

Control Assessment Process

NIST SP 800-53A provides a repeatable process to **prepare** for, **develop plans** for, and **conduct** control assessments, and **analyze** assessment results as part of a risk management process



Prepare for Security and Privacy Control Assessments

Develop Security and Privacy Assessment Plans

Conduct Security and Privacy Control Assessments

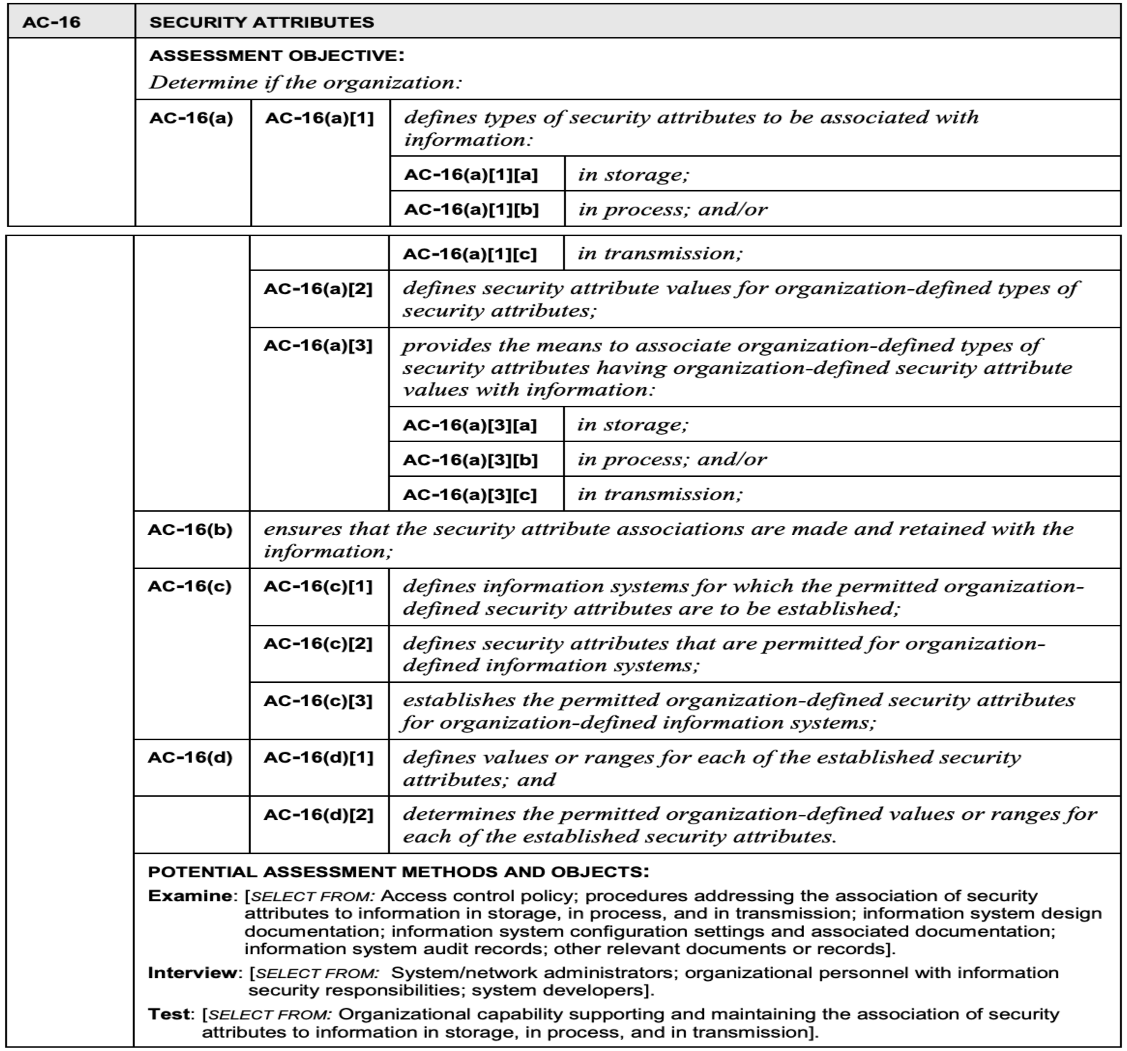
Analyze Assessment Report Results

Each Step (Prepare, Develop, Conduct, Analyze) includes:

Purpose ◆ *Primary and Supporting Roles* ◆ Outcomes ◆ In-depth Tasks and Guidance

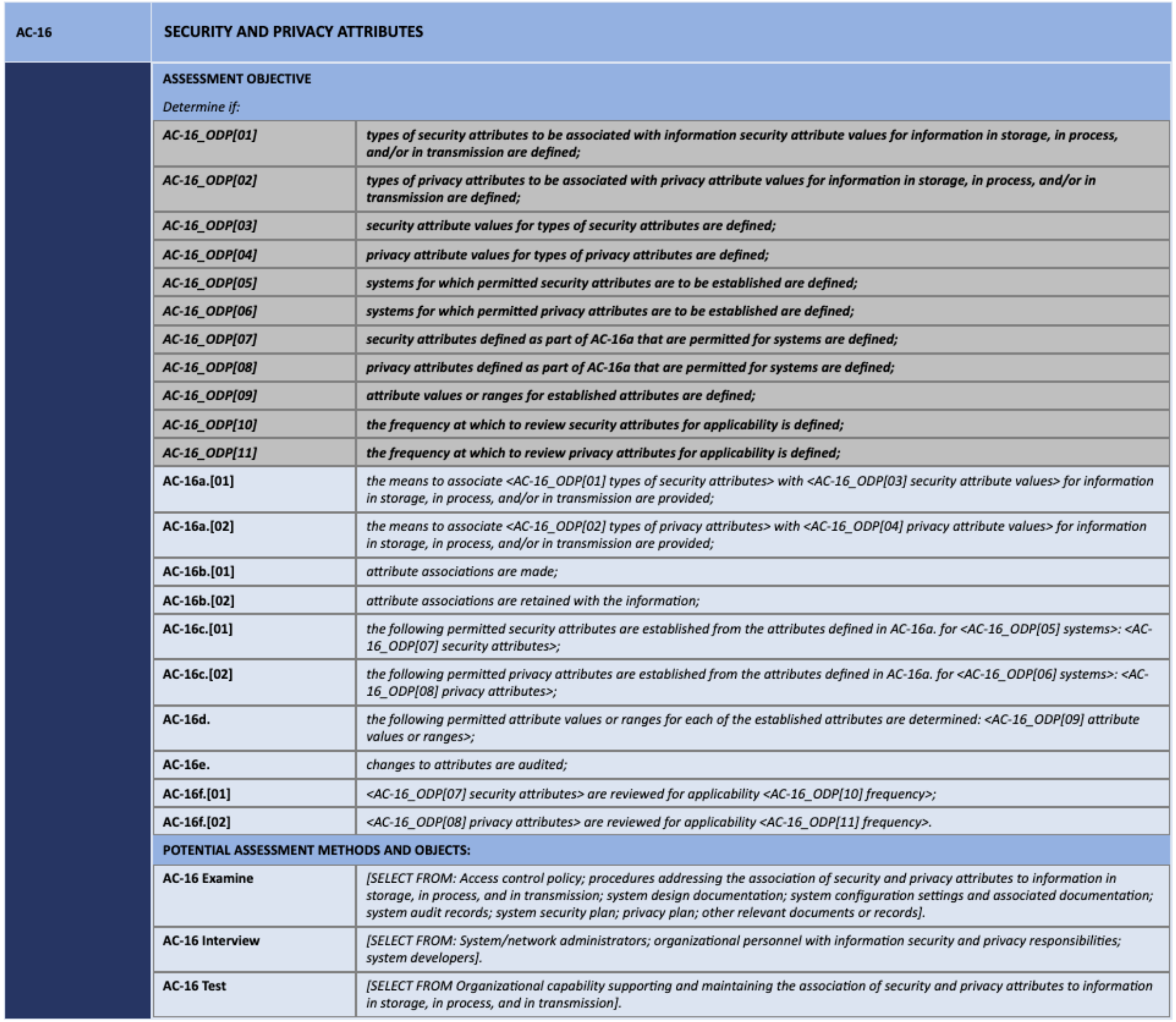
Sample SP 800-53A Assessment Procedure: Revision 4 vs. Revision 5

SP 800-53A Rev 4 (2014)



AC-16	SECURITY ATTRIBUTES			
	ASSESSMENT OBJECTIVE: *Determine if the organization:*			
	AC-16(a)	**AC-16(a)[1]**	*defines types of security attributes to be associated with information:*	
			AC-16(a)[1][a]	*in storage;*
			AC-16(a)[1][b]	*in process; and/or*
			AC-16(a)[1][c]	*in transmission;*
		AC-16(a)[2]	*defines security attribute values for organization-defined types of security attributes;*	
		AC-16(a)[3]	*provides the means to associate organization-defined types of security attributes having organization-defined security attribute values with information:*	
			AC-16(a)[3][a]	*in storage;*
			AC-16(a)[3][b]	*in process; and/or*
			AC-16(a)[3][c]	*in transmission;*
	AC-16(b)	*ensures that the security attribute associations are made and retained with the information;*		
	AC-16(c)	**AC-16(c)[1]**	*defines information systems for which the permitted organization-defined security attributes are to be established;*	
		AC-16(c)[2]	*defines security attributes that are permitted for organization-defined information systems;*	
		AC-16(c)[3]	*establishes the permitted organization-defined security attributes for organization-defined information systems;*	
	AC-16(d)	**AC-16(d)[1]**	*defines values or ranges for each of the established security attributes; and*	
		AC-16(d)[2]	*determines the permitted organization-defined values or ranges for each of the established security attributes.*	
	POTENTIAL ASSESSMENT METHODS AND OBJECTS: **Examine**: [*SELECT FROM:* Access control policy; procedures addressing the association of security attributes to information in storage, in process, and in transmission; information system design documentation; information system configuration settings and associated documentation; information system audit records; other relevant documents or records]. **Interview**: [*SELECT FROM:* System/network administrators; organizational personnel with information security responsibilities; system developers]. **Test**: [*SELECT FROM:* Organizational capability supporting and maintaining the association of security attributes to information in storage, in process, and in transmission].			

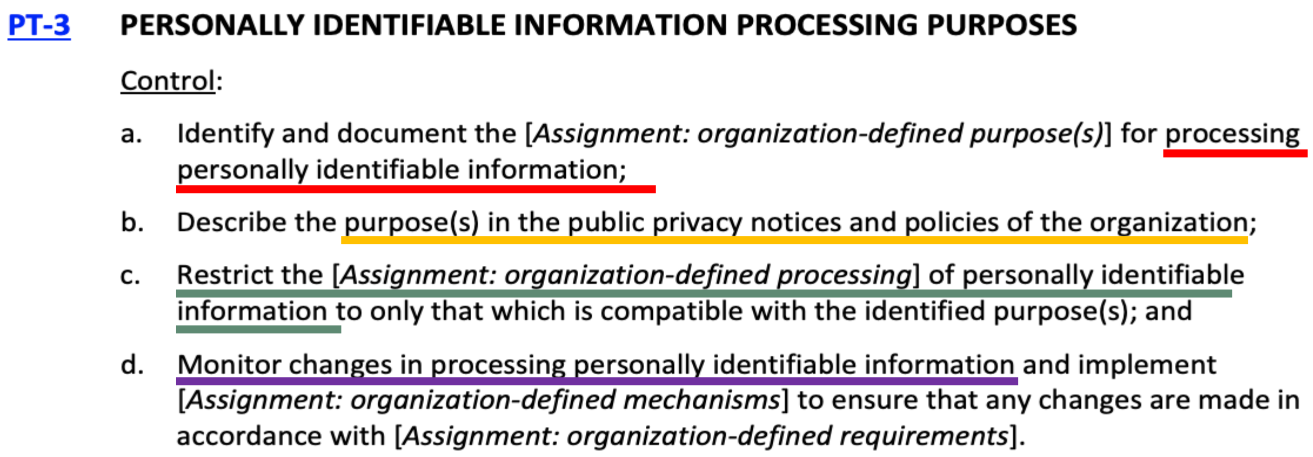
SP 800-53A Rev 5 (2022)



AC-16	SECURITY AND PRIVACY ATTRIBUTES	
	ASSESSMENT OBJECTIVE *Determine if:*	
	AC-16_ODP[01]	***types of security attributes to be associated with information security attribute values for information in storage, in process, and/or in transmission are defined;***
	AC-16_ODP[02]	***types of privacy attributes to be associated with privacy attribute values for information in storage, in process, and/or in transmission are defined;***
	AC-16_ODP[03]	***security attribute values for types of security attributes are defined;***
	AC-16_ODP[04]	***privacy attribute values for types of privacy attributes are defined;***
	AC-16_ODP[05]	***systems for which permitted security attributes are to be established are defined;***
	AC-16_ODP[06]	***systems for which permitted privacy attributes are to be established are defined;***
	AC-16_ODP[07]	***security attributes defined as part of AC-16a that are permitted for systems are defined;***
	AC-16_ODP[08]	***privacy attributes defined as part of AC-16a that are permitted for systems are defined;***
	AC-16_ODP[09]	***attribute values or ranges for established attributes are defined;***
	AC-16_ODP[10]	***the frequency at which to review security attributes for applicability is defined;***
	AC-16_ODP[11]	***the frequency at which to review privacy attributes for applicability is defined;***
	AC-16a.[01]	*the means to associate <AC-16_ODP[01] types of security attributes> with <AC-16_ODP[03] security attribute values> for information in storage, in process, and/or in transmission are provided;*
	AC-16a.[02]	*the means to associate <AC-16_ODP[02] types of privacy attributes> with <AC-16_ODP[04] privacy attribute values> for information in storage, in process, and/or in transmission are provided;*
	AC-16b.[01]	*attribute associations are made;*
	AC-16b.[02]	*attribute associations are retained with the information;*
	AC-16c.[01]	*the following permitted security attributes are established from the attributes defined in AC-16a. for <AC-16_ODP[05] systems>: <AC-16_ODP[07] security attributes>;*
	AC-16c.[02]	*the following permitted privacy attributes are established from the attributes defined in AC-16a. for <AC-16_ODP[06] systems>: <AC-16_ODP[08] privacy attributes>;*
	AC-16d.	*the following permitted attribute values or ranges for each of the established attributes are determined: <AC-16_ODP[09] attribute values or ranges>;*
	AC-16e.	*changes to attributes are audited;*
	AC-16f.[01]	*<AC-16_ODP[07] security attributes> are reviewed for applicability <AC-16_ODP[10] frequency>;*
	AC-16f.[02]	*<AC-16_ODP[08] privacy attributes> are reviewed for applicability <AC-16_ODP[11] frequency>.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	AC-16 Examine	*[SELECT FROM: Access control policy; procedures addressing the association of security and privacy attributes to information in storage, in process, and in transmission; system design documentation; system configuration settings and associated documentation; system audit records; system security plan; privacy plan; other relevant documents or records].*
	AC-16 Interview	*[SELECT FROM: System/network administrators; organizational personnel with information security and privacy responsibilities; system developers].*
	AC-16 Test	*[SELECT FROM Organizational capability supporting and maintaining the association of security and privacy attributes to information in storage, in process, and in transmission].*

Assessment Procedure Schema: Relationship between 53 and 53A

NIST SPECIAL PUBLICATION
SP 800-53
53
REVISION 5
SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS
RISK MANAGEMENT FRAMEWORK



PT-3 **PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES**

Control:

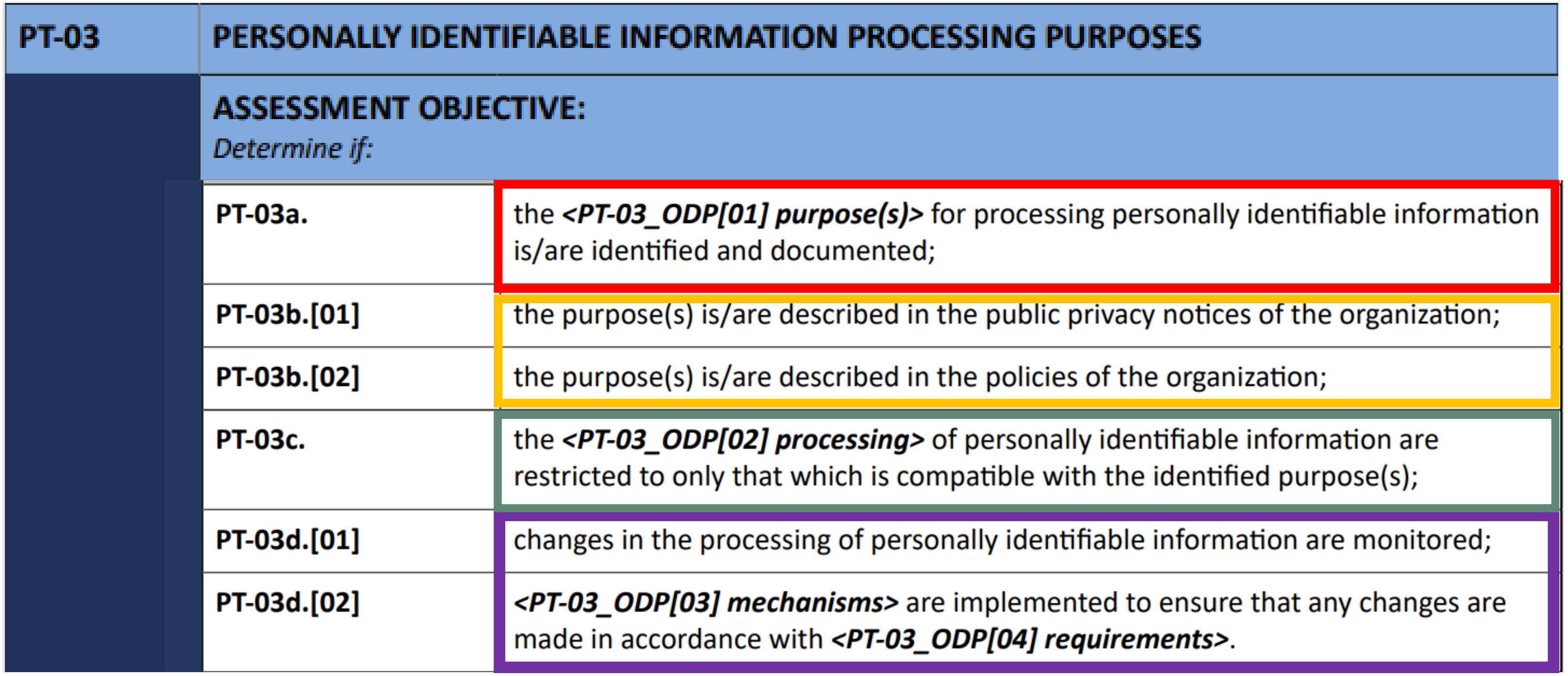
a. Identify and document the [*Assignment: organization-defined purpose(s)*] for processing personally identifiable information;

b. Describe the purpose(s) in the public privacy notices and policies of the organization;

c. Restrict the [*Assignment: organization-defined processing*] of personally identifiable information to only that which is compatible with the identified purpose(s); and

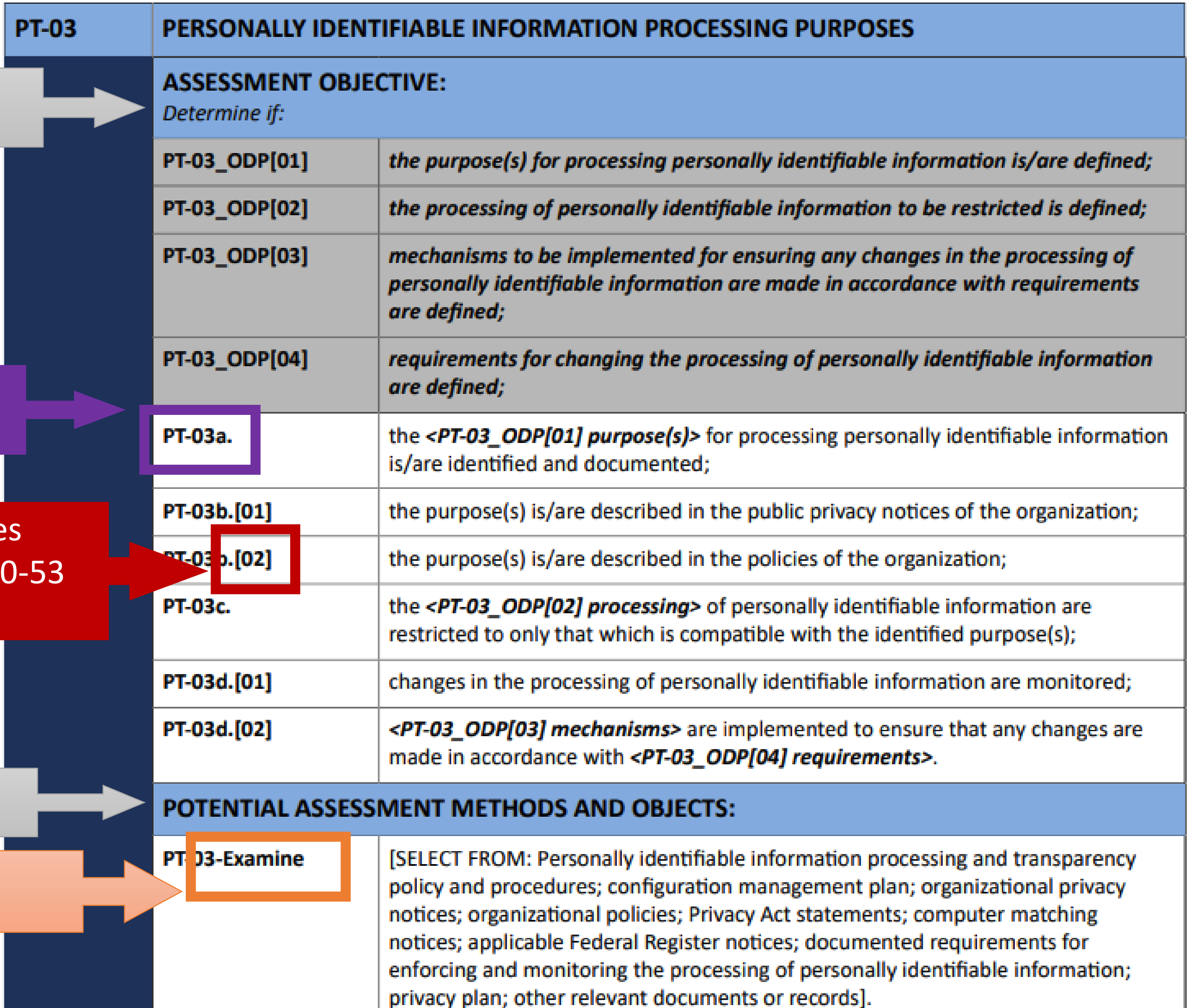
d. Monitor changes in processing personally identifiable information and implement [*Assignment: organization-defined mechanisms*] to ensure that any changes are made in accordance with [*Assignment: organization-defined requirements*].

NIST SPECIAL PUBLICATION
SP 800-53A
53A
REVISION 5
ASSESSING SECURITY AND PRIVACY CONTROLS IN INFORMATION SYSTEMS AND ORGANIZATIONS
RISK MANAGEMENT FRAMEWORK



PT-03	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-03a.	the ***<PT-03_ODP[01] purpose(s)>*** for processing personally identifiable information is/are identified and documented;
	PT-03b.[01]	the purpose(s) is/are described in the public privacy notices of the organization;
	PT-03b.[02]	the purpose(s) is/are described in the policies of the organization;
	PT-03c.	the ***<PT-03_ODP[02] processing>*** of personally identifiable information are restricted to only that which is compatible with the identified purpose(s);
	PT-03d.[01]	changes in the processing of personally identifiable information are monitored;
	PT-03d.[02]	***<PT-03_ODP[03] mechanisms>*** are implemented to ensure that any changes are made in accordance with ***<PT-03_ODP[04] requirements>***.

Assessment Procedure Schema: Controls



PT-03	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES	
	ASSESSMENT OBJECTIVE: *Determine if:*	
	PT-03_ODP[01]	*the purpose(s) for processing personally identifiable information is/are defined;*
	PT-03_ODP[02]	*the processing of personally identifiable information to be restricted is defined;*
	PT-03_ODP[03]	*mechanisms to be implemented for ensuring any changes in the processing of personally identifiable information are made in accordance with requirements are defined;*
	PT-03_ODP[04]	*requirements for changing the processing of personally identifiable information are defined;*
	PT-03a.	the ***<PT-03_ODP[01] purpose(s)>*** for processing personally identifiable information is/are identified and documented;
	PT-03b.[01]	the purpose(s) is/are described in the public privacy notices of the organization;
	PT-03b.[02]	the purpose(s) is/are described in the policies of the organization;
	PT-03c.	the ***<PT-03_ODP[02] processing>*** of personally identifiable information are restricted to only that which is compatible with the identified purpose(s);
	PT-03d.[01]	changes in the processing of personally identifiable information are monitored;
	PT-03d.[02]	***<PT-03_ODP[03] mechanisms>*** are implemented to ensure that any changes are made in accordance with ***<PT-03_ODP[04] requirements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:	
	PT-03-Examine	[SELECT FROM: Personally identifiable information processing and transparency policy and procedures; configuration management plan; organizational privacy notices; organizational policies; Privacy Act statements; computer matching notices; applicable Federal Register notices; documented requirements for enforcing and monitoring the processing of personally identifiable information; privacy plan; other relevant documents or records].

Assessment Objectives

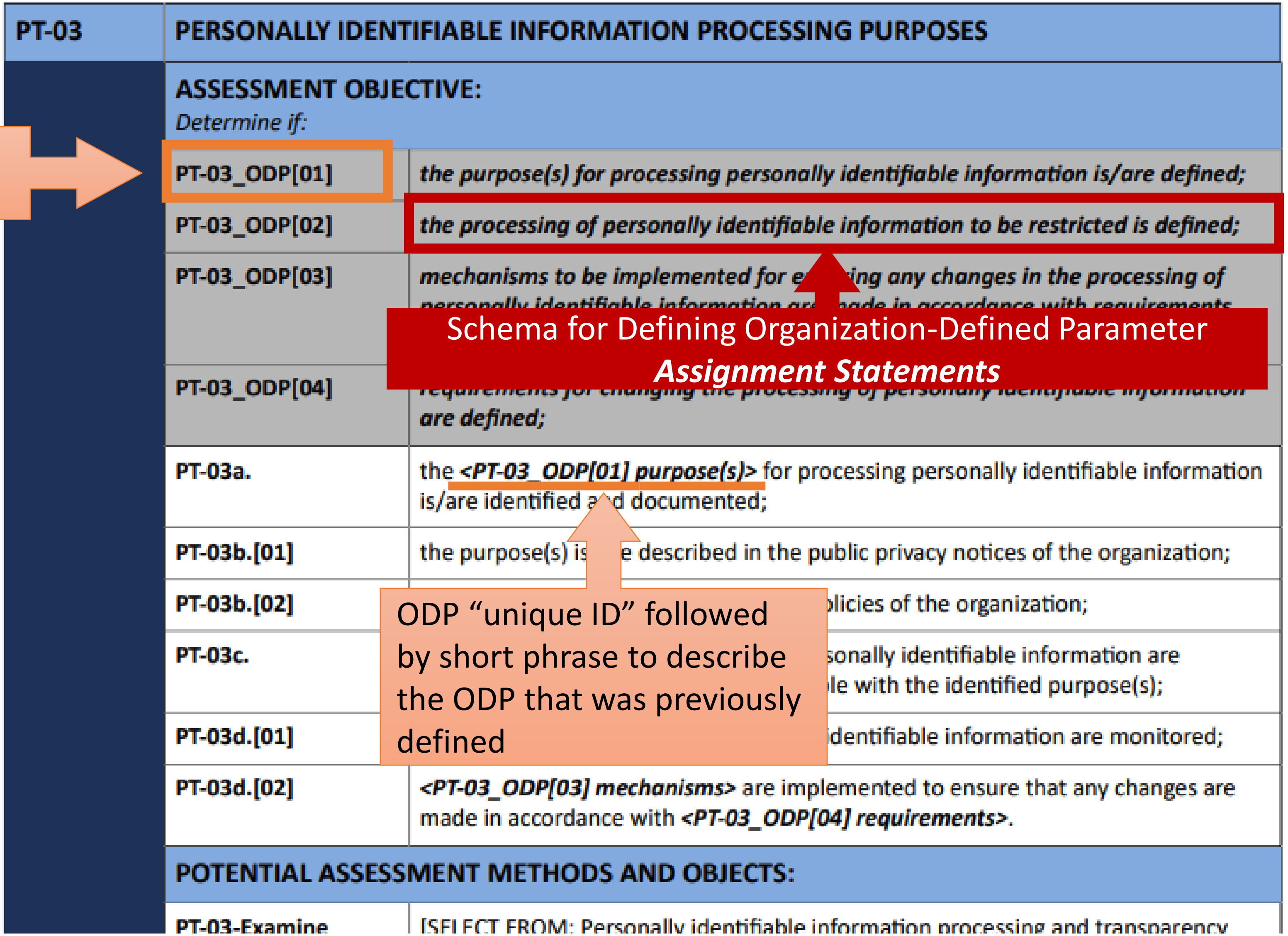
Corresponds directly with SP 800-53 control item

Bracketed numbers indicates granularization from the SP 800-53 control item.

Potential Methods & Objects

Control ID "Tag" for Potential Methods

Assessment Procedure Schema: Organization-Defined Parameters (ODP)



PT-03	PERSONALLY IDENTIFIABLE INFORMATION PROCESSING PURPOSES
	ASSESSMENT OBJECTIVE: *Determine if:*
PT-03_ODP[01]	***the purpose(s) for processing personally identifiable information is/are defined;***
PT-03_ODP[02]	***the processing of personally identifiable information to be restricted is defined;***
PT-03_ODP[03]	***mechanisms to be implemented for e ing any changes in the processing of personally identifiable information ar ade in accordance with requirements***
PT-03_ODP[04]	***requirements for changing the processing of personally identifiable information are defined;***
PT-03a.	the ***<PT-03_ODP[01] purpose(s)>*** for processing personally identifiable information is/are identified a d documented;
PT-03b.[01]	the purpose(s) is e described in the public privacy notices of the organization;
PT-03b.[02]	licies of the organization;
PT-03c.	sonally identifiable information are le with the identified purpose(s);
PT-03d.[01]	identifiable information are monitored;
PT-03d.[02]	***<PT-03_ODP[03] mechanisms>*** are implemented to ensure that any changes are made in accordance with ***<PT-03_ODP[04] requirements>***.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
PT-03-Examine	[SELECT FROM: Personally identifiable information processing and transparency

Organization-defined Parameters "unique ID"

Schema for Defining Organization-Defined Parameter ***Assignment Statements***

ODP "unique ID" followed by short phrase to describe the ODP that was previously defined

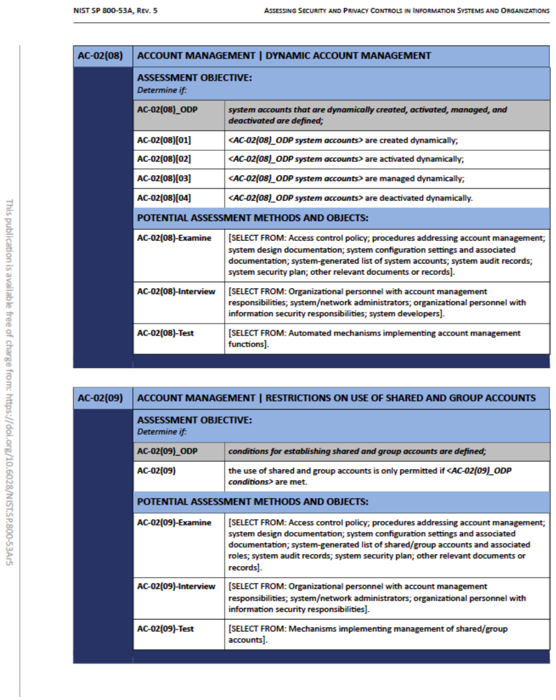
Available in Multiple Data Formats

PDF

CSV

TXT

OSCAL

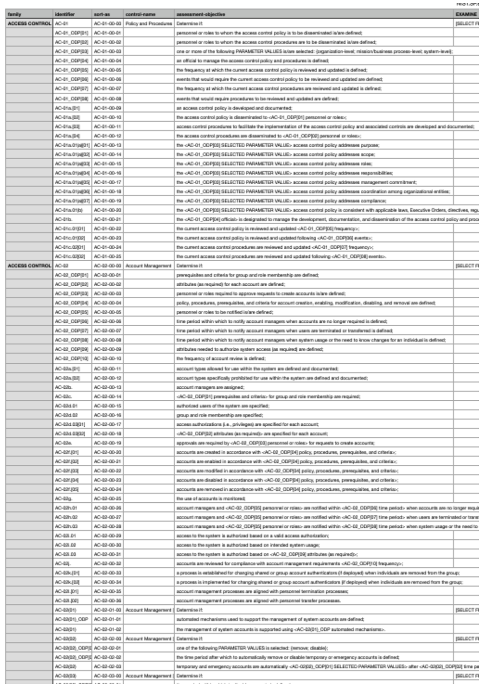


NIST SP 800-53A, Rev. 5 — Assessing Security and Privacy Controls in Information Systems and Organizations

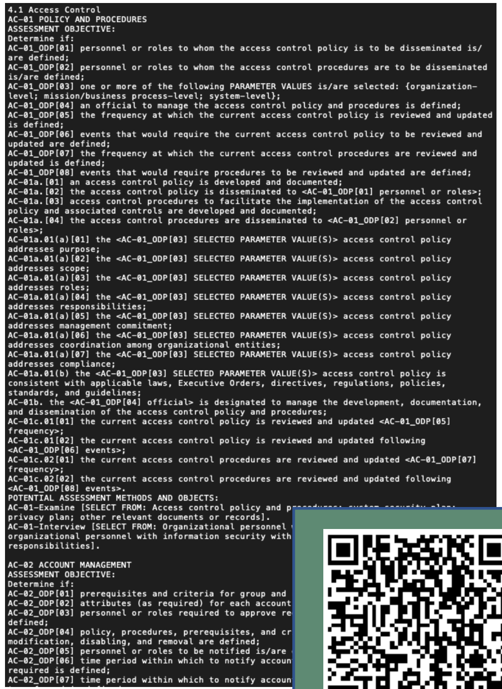
This publication is available free of charge from: https://doi.org/10.6028/NIST.SP.800-53Ar5

AC-02(08)	ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT MANAGEMENT
	ASSESSMENT OBJECTIVE: *Determine if:*
AC-02(08)_ODP	***system accounts that are dynamically created, activated, managed, and deactivated are defined;***
AC-02(08)[01]	*<AC-02(08)_ODP system accounts>* are created dynamically;
AC-02(08)[02]	*<AC-02(08)_ODP system accounts>* are activated dynamically;
AC-02(08)[03]	*<AC-02(08)_ODP system accounts>* are managed dynamically;
AC-02(08)[04]	*<AC-02(08)_ODP system accounts>* are deactivated dynamically.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
AC-02(08)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of system accounts; system audit records; system security plan; other relevant documents or records].
AC-02(08)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities; system developers].
AC-02(08)-Test	[SELECT FROM: Automated mechanisms implementing account management functions].

AC-02(09)	ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS
	ASSESSMENT OBJECTIVE: *Determine if:*
AC-02(09)_ODP	***conditions for establishing shared and group accounts are defined;***
AC-02(09)	the use of shared and group accounts is only permitted if ***<AC-02(09)_ODP conditions>*** are met.
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
AC-02(09)-Examine	[SELECT FROM: Access control policy; procedures addressing account management; system design documentation; system configuration settings and associated documentation; system-generated list of shared/group accounts and associated roles; system audit records; system security plan; other relevant documents or records].
AC-02(09)-Interview	[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security responsibilities].
AC-02(09)-Test	[SELECT FROM: Mechanisms implementing management of shared/group accounts].

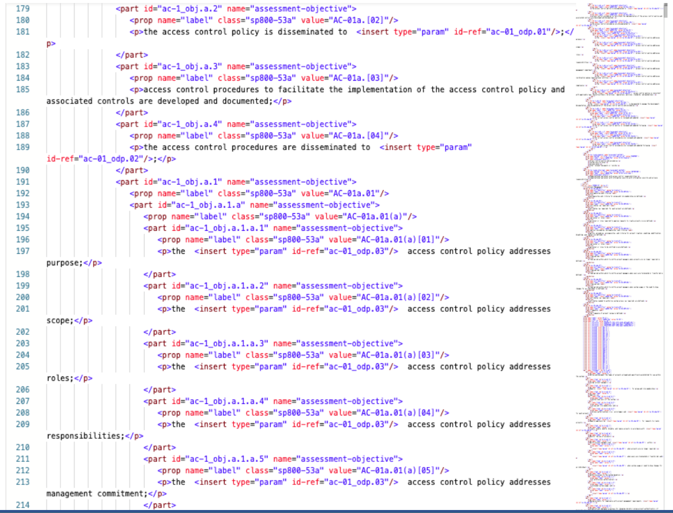


family	identifier	sort-as	control-name	assessment-objective	EXAMINE
ACCESS CONTROL	AC-01	AC-01-00-00	Policy and Procedures	Determine if:	[SELECT FI
	AC-01_ODP[01]	AC-01-00-01		personnel or roles to whom the access control policy is to be disseminated is/are defined;	
	AC-01_ODP[02]	AC-01-00-02		personnel or roles to whom the access control procedures are to be disseminated is/are defined;	
	AC-01_ODP[03]	AC-01-00-03		one or more of the following PARAMETER VALUES is/are selected: {organization-level; mission/business process-level; system-level};	
	AC-01_ODP[04]	AC-01-00-04		an official to manage the access control policy and procedures is defined;	
	AC-01_ODP[05]	AC-01-00-05		the frequency at which the current access control policy is reviewed and updated is defined;	
	AC-01_ODP[06]	AC-01-00-06		events that would require the current access control policy to be reviewed and updated are defined;	
	AC-01_ODP[07]	AC-01-00-07		the frequency at which the current access control procedures are reviewed and updated is defined;	
	AC-01_ODP[08]	AC-01-00-08		events that would require procedures to be reviewed and updated are defined;	
	AC-01a.[01]	AC-01-00-09		an access control policy is developed and documented;	
	AC-01a.[02]	AC-01-00-10		the access control policy is disseminated to <AC-01_ODP[01] personnel or roles>;	
	AC-01a.[03]	AC-01-00-11		access control procedures to facilitate the implementation of the access control policy and associated controls are developed and documented;	
	AC-01a.[04]	AC-01-00-12		the access control procedures are disseminated to <AC-01_ODP[02] personnel or roles>;	
	AC-01a.01(a)[01]	AC-01-00-13		the <AC-01_ODP[03] SELECTED PARAMETER VALUE> access control policy addresses purpose;	
	AC-01a.01(a)[02]	AC-01-00-14		the <AC-01_ODP[03] SELECTED PARAMETER VALUE> access control policy addresses scope;	
	AC-01a.01(a)[03]	AC-01-00-15		the <AC-01_ODP[03] SELECTED PARAMETER VALUE> access control policy addresses roles;	
	AC-01a.01(a)[04]	AC-01-00-16		the <AC-01_ODP[03] SELECTED PARAMETER VALUE> access control policy addresses responsibilities;	
	AC-01a.01(a)[05]	AC-01-00-17		the <AC-01_ODP[03] SELECTED PARAMETER VALUE> access control policy addresses management commitment;	
	AC-01a.01(a)[06]	AC-01-00-18		the <AC-01_ODP[03] SELECTED PARAMETER VALUE> access control policy addresses coordination among organizational entities;	
	AC-01a.01(a)[07]	AC-01-00-19		the <AC-01_ODP[03] SELECTED PARAMETER VALUE> access control policy addresses compliance;	
	AC-01a.01(b)	AC-01-00-20		the <AC-01_ODP[03] SELECTED PARAMETER VALUE> access control policy is consistent with applicable laws, Executive Orders, directives, regu	
	AC-01b.	AC-01-00-21		the <AC-01_ODP[04] official> is designated to manage the development, documentation, and dissemination of the access control policy and proc	
	AC-01c.01[01]	AC-01-00-22		the current access control policy is reviewed and updated <AC-01_ODP[05] frequency>;	
	AC-01c.01[02]	AC-01-00-23		the current access control policy is reviewed and updated following <AC-01_ODP[06] events>;	
	AC-01c.02[01]	AC-01-00-24		the current access control procedures are reviewed and updated <AC-01_ODP[07] frequency>;	
	AC-01c.02[02]	AC-01-00-25		the current access control procedures are reviewed and updated following <AC-01_ODP[08] events>.	
ACCESS CONTROL	AC-02	AC-02-00-00	Account Management	Determine if:	[SELECT FI
	AC-02_ODP[01]	AC-02-00-01		prerequisites and criteria for group and role membership are defined;	
	AC-02_ODP[02]	AC-02-00-02		attributes (as required) for each account are defined;	
	AC-02_ODP[03]	AC-02-00-03		personnel or roles required to approve requests to create accounts is/are defined;	
	AC-02_ODP[04]	AC-02-00-04		policy, procedures, prerequisites, and criteria for account creation, enabling, modification, disabling, and removal are defined;	
	AC-02_ODP[05]	AC-02-00-05		personnel or roles to be notified is/are defined;	
	AC-02_ODP[06]	AC-02-00-06		time period within which to notify account managers when accounts are no longer required is defined;	
	AC-02_ODP[07]	AC-02-00-07		time period within which to notify account managers when users are terminated or transferred is defined;	
	AC-02_ODP[08]	AC-02-00-08		time period within which to notify account managers when system usage or the need to know changes for an individual is defined;	
	AC-02_ODP[09]	AC-02-00-09		attributes needed to authorize system access (as required) are defined;	
	AC-02_ODP[10]	AC-02-00-10		the frequency of account review is defined;	
	AC-02a.[01]	AC-02-00-11		account types allowed for use within the system are defined and documented;	
	AC-02a.[02]	AC-02-00-12		account types specifically prohibited for use within the system are defined and documented;	
	AC-02b.	AC-02-00-13		account managers are assigned;	
	AC-02c.	AC-02-00-14		<AC-02_ODP[01] prerequisites and criteria> for group and role membership are required;	
	AC-02d.01	AC-02-00-15		authorized users of the system are specified;	
	AC-02d.02	AC-02-00-16		group and role membership are specified;	
	AC-02d.03[01]	AC-02-00-17		access authorizations (i.e., privileges) are specified for each account;	
	AC-02d.03[02]	AC-02-00-18		<AC-02_ODP[02] attributes (as required)> are specified for each account;	
	AC-02e.	AC-02-00-19		approvals are required by <AC-02_ODP[03] personnel or roles> for requests to create accounts;	
	AC-02f.[01]	AC-02-00-20		accounts are created in accordance with <AC-02_ODP[04] policy, procedures, prerequisites, and criteria>;	
	AC-02f.[02]	AC-02-00-21		accounts are enabled in accordance with <AC-02_ODP[04] policy, procedures, prerequisites, and criteria>;	
	AC-02f.[03]	AC-02-00-22		accounts are modified in accordance with <AC-02_ODP[04] policy, procedures, prerequisites, and criteria>;	
	AC-02f.[04]	AC-02-00-23		accounts are disabled in accordance with <AC-02_ODP[04] policy, procedures, prerequisites, and criteria>;	
	AC-02f.[05]	AC-02-00-24		accounts are removed in accordance with <AC-02_ODP[04] policy, procedures, prerequisites, and criteria>;	
	AC-02g.	AC-02-00-25		the use of accounts is monitored;	
	AC-02h.01	AC-02-00-26		account managers and <AC-02_ODP[05] personnel or roles> are notified within <AC-02_ODP[06] time period> when accounts are no longer requi	
	AC-02h.02	AC-02-00-27		account managers and <AC-02_ODP[05] personnel or roles> are notified within <AC-02_ODP[07] time period> when users are terminated or trans	
	AC-02h.03	AC-02-00-28		account managers and <AC-02_ODP[05] personnel or roles> are notified within <AC-02_ODP[08] time period> when system usage or the need to	
	AC-02i.01	AC-02-00-29		access to the system is authorized based on a valid access authorization;	
	AC-02i.02	AC-02-00-30		access to the system is authorized based on intended system usage;	
	AC-02i.03	AC-02-00-31		access to the system is authorized based on <AC-02_ODP[09] attributes (as required)>;	
	AC-02j.	AC-02-00-32		accounts are reviewed for compliance with account management requirements <AC-02_ODP[10] frequency>;	
	AC-02k.[01]	AC-02-00-33		a process is established for changing shared or group account authenticators (if deployed) when individuals are removed from the group;	
	AC-02k.[02]	AC-02-00-34		a process is implemented for changing shared or group account authenticators (if deployed) when individuals are removed from the group;	
	AC-02l.[01]	AC-02-00-35		account management processes are aligned with personnel termination processes;	
	AC-02l.[02]	AC-02-00-36		account management processes are aligned with personnel transfer processes.	
	AC-02(01)	AC-02-01-00	Account Management |	Determine if:	[SELECT FI
	AC-02(01)_ODP	AC-02-01-01		automated mechanisms used to support the management of system accounts are defined;	
	AC-02(01)	AC-02-01-02		the management of system accounts is supported using <AC-02(01)_ODP automated mechanisms>.	
	AC-02(02)	AC-02-02-00	Account Management |	Determine if:	[SELECT FI
	AC-02(02)_ODP[0	AC-02-02-01		one of the following PARAMETER VALUES is selected: {remove; disable};	
	AC-02(02)_ODP[0	AC-02-02-02		the time period after which to automatically remove or disable temporary or emergency accounts is defined;	
	AC-02(02)	AC-02-02-03		temporary and emergency accounts are automatically <AC-02(02)_ODP[01] SELECTED PARAMETER VALUES> after <AC-02(02)_ODP[02] time pe	
	AC-02(03)	AC-02-03-00	Account Management |	Determine if:	[SELECT FI



```
4.1 Access Control
AC-01 POLICY AND PROCEDURES
ASSESSMENT OBJECTIVE:
Determine if:
AC-01_ODP[01] personnel or roles to whom the access control policy is to be disseminated is/
are defined;
AC-01_ODP[02] personnel or roles to whom the access control procedures are to be disseminated
is/are defined;
AC-01_ODP[03] one or more of the following PARAMETER VALUES is/are selected: {organization-
level; mission/business process-level; system-level};
AC-01_ODP[04] an official to manage the access control policy and procedures is defined;
AC-01_ODP[05] the frequency at which the current access control policy is reviewed and updated
is defined;
AC-01_ODP[06] events that would require the current access control policy to be reviewed and
updated are defined;
AC-01_ODP[07] the frequency at which the current access control procedures are reviewed and
updated is defined;
AC-01_ODP[08] events that would require procedures to be reviewed and updated are defined;
AC-01a.[01] an access control policy is developed and documented;
AC-01a.[02] the access control policy is disseminated to <AC-01_ODP[01] personnel or roles>;
AC-01a.[03] access control procedures to facilitate the implementation of the access control
policy and associated controls are developed and documented;
AC-01a.[04] the access control procedures are disseminated to <AC-01_ODP[02] personnel or
roles>;
AC-01a.01(a)[01] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy
addresses purpose;
AC-01a.01(a)[02] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy
addresses scope;
AC-01a.01(a)[03] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy
addresses roles;
AC-01a.01(a)[04] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy
addresses responsibilities;
AC-01a.01(a)[05] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy
addresses management commitment;
AC-01a.01(a)[06] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy
addresses coordination among organizational entities;
AC-01a.01(a)[07] the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy
addresses compliance;
AC-01a.01(b) the <AC-01_ODP[03] SELECTED PARAMETER VALUE(S)> access control policy is
consistent with applicable laws, Executive Orders, directives, regulations, policies,
standards, and guidelines;
AC-01b. the <AC-01_ODP[04] official> is designated to manage the development, documentation,
and dissemination of the access control policy and procedures;
AC-01c.01[01] the current access control policy is reviewed and updated <AC-01_ODP[05]
frequency>;
AC-01c.01[02] the current access control policy is reviewed and updated following
<AC-01_ODP[06] events>;
AC-01c.02[01] the current access control procedures are reviewed and updated <AC-01_ODP[07]
frequency>;
AC-01c.02[02] the current access control procedures are reviewed and updated following
<AC-01_ODP[08] events>.
POTENTIAL ASSESSMENT METHODS AND OBJECTS:
AC-01-Examine [SELECT FROM: Access control policy and procedures; system security plan;
privacy plan; other relevant documents or records].
AC-01-Interview [SELECT FROM: Organizational personnel with
organizational personnel with information security with
responsibilities].

AC-02 ACCOUNT MANAGEMENT
ASSESSMENT OBJECTIVE:
Determine if:
AC-02_ODP[01] prerequisites and criteria for group and
AC-02_ODP[02] attributes (as required) for each account
AC-02_ODP[03] personnel or roles required to approve re
defined;
AC-02_ODP[04] policy, procedures, prerequisites, and cr
modification, disabling, and removal are defined;
AC-02_ODP[05] personnel or roles to be notified is/are
AC-02_ODP[06] time period within which to notify accoun
required is defined;
AC-02_ODP[07] time period within which to notify accoun
```



```
            <part id="ac-1_obj.a.2" name="assessment-objective">
              <prop name="label" class="sp800-53a" value="AC-01a.[02]"/>
              <p>the access control policy is disseminated to  <insert type="param" id-ref="ac-01_odp.01"/>;</p>
            </part>
            <part id="ac-1_obj.a.3" name="assessment-objective">
              <prop name="label" class="sp800-53a" value="AC-01a.[03]"/>
              <p>access control procedures to facilitate the implementation of the access control policy and associated controls are developed and documented;</p>
            </part>
            <part id="ac-1_obj.a.4" name="assessment-objective">
              <prop name="label" class="sp800-53a" value="AC-01a.[04]"/>
              <p>the access control procedures are disseminated to  <insert type="param" id-ref="ac-01_odp.02"/>;</p>
            </part>
            <part id="ac-1_obj.a.1" name="assessment-objective">
              <prop name="label" class="sp800-53a" value="AC-01a.01"/>
              <part id="ac-1_obj.a.1.a" name="assessment-objective">
                <prop name="label" class="sp800-53a" value="AC-01a.01(a)"/>
                <part id="ac-1_obj.a.1.a.1" name="assessment-objective">
                  <prop name="label" class="sp800-53a" value="AC-01a.01(a)[01]"/>
                  <p>the  <insert type="param" id-ref="ac-01_odp.03"/>  access control policy addresses purpose;</p>
                </part>
                <part id="ac-1_obj.a.1.a.2" name="assessment-objective">
                  <prop name="label" class="sp800-53a" value="AC-01a.01(a)[02]"/>
                  <p>the  <insert type="param" id-ref="ac-01_odp.03"/>  access control policy addresses scope;</p>
                </part>
                <part id="ac-1_obj.a.1.a.3" name="assessment-objective">
                  <prop name="label" class="sp800-53a" value="AC-01a.01(a)[03]"/>
                  <p>the  <insert type="param" id-ref="ac-01_odp.03"/>  access control policy addresses roles;</p>
                </part>
                <part id="ac-1_obj.a.1.a.4" name="assessment-objective">
                  <prop name="label" class="sp800-53a" value="AC-01a.01(a)[04]"/>
                  <p>the  <insert type="param" id-ref="ac-01_odp.03"/>  access control policy addresses responsibilities;</p>
                </part>
                <part id="ac-1_obj.a.1.a.5" name="assessment-objective">
                  <prop name="label" class="sp800-53a" value="AC-01a.01(a)[05]"/>
                  <p>the  <insert type="param" id-ref="ac-01_odp.03"/>  access control policy addresses management commitment;</p>
                </part>
```

CSV, TXT and OSCAL available under “Supplemental Material”

Looking Ahead for NIST SP 800-53

SP 800-53 Comment Site Now Available!

- Submit your comments & ideas on SP 800-53/53B
- https://csrc.nist.gov/Projects/risk-management/sp800-53-controls

The NIST RMF Team is already planning for Revision 6

- **No planned date for Revision 6 yet!**
- *For Revision 6*, NIST will release **draft controls, draft control baselines**, and **draft control assessment procedures concurrently**

SIMPLIFY| INNOVATE | AUTOMATE

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

STAY IN TOUCH

CONTACT US

nist.gov/RMF

@NISTcyber

sec-cert@nist.gov

privacy-eng@nist.gov

Back-up slides

Resources

Computer Security Resource Center (CSRC) email updates
https://public.govdelivery.com/accounts/USNIST/subscriber/new?qsp=USNIST_3

NIST Risk Management Framework (RMF) (FISMA Implementation) Project Mailing List (announce list)
https://csrc.nist.gov/Projects/risk-management/mailing-list

Drafts Open for Comment
https://csrc.nist.gov/publications/drafts-open-for-comment

NIST Security and Privacy Control Overlay Repository (SCOR)
https://csrc.nist.gov/Projects/Risk-Management/scor

NIST National Cybersecurity Center of Excellence (NCCoE)
https://www.nccoe.nist.gov

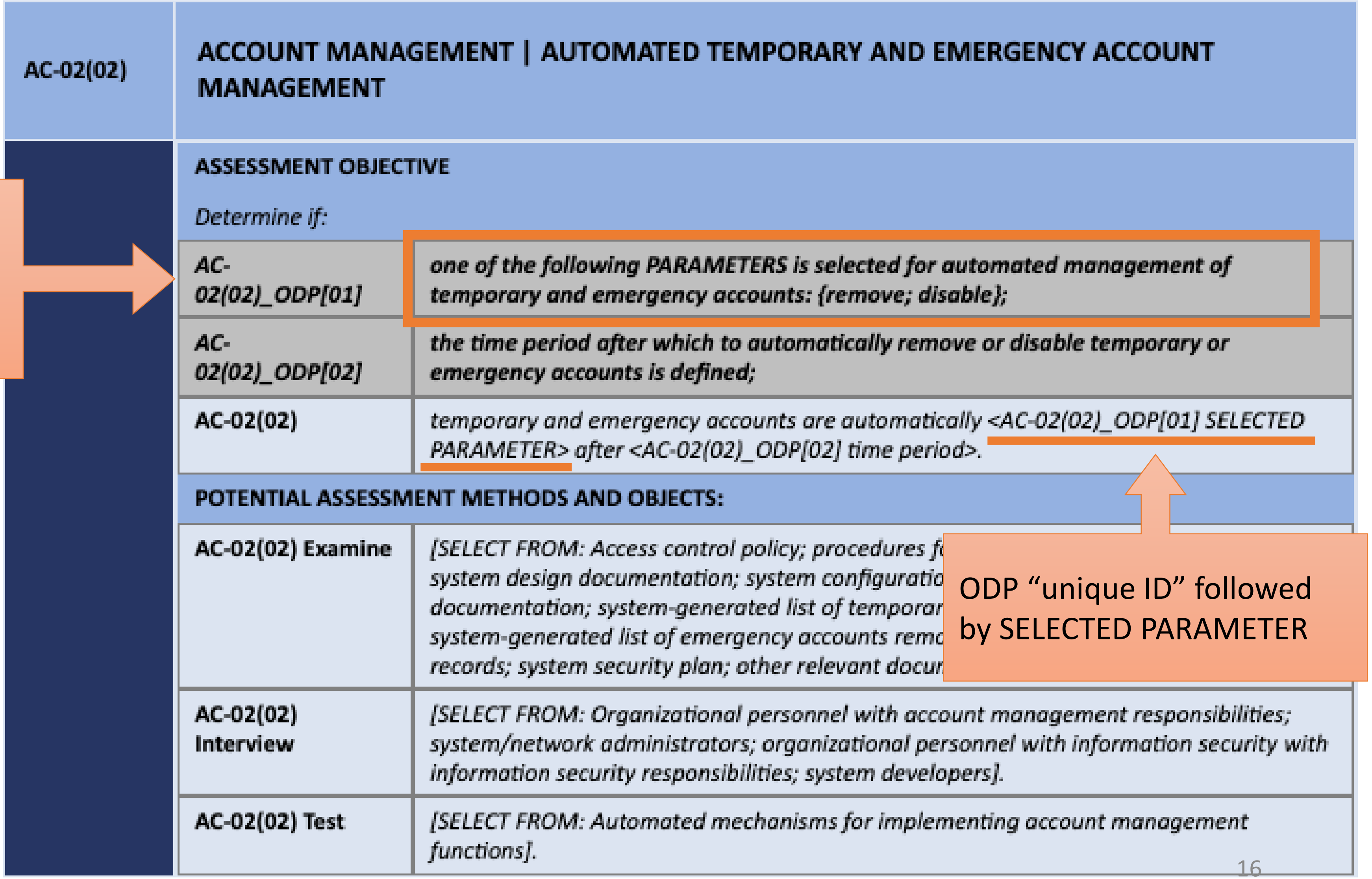
NIST SP 800-53 Control and Control Baseline Release Search Site + Public Comment Site
https://nist.gov/rmf/sp800-53-controls

Future Revisions of SP 800-53: Release Criteria

Change Type	Minor Release	Major Release
Correct error in punctuation, spelling, or grammar that does not impact technical implementation	X	
Correct other error that does not impact technical implementation	X	
Add new control or control enhancement not in control baseline	X	
Add control or control enhancement to a control baseline (existing or new control)		X
Remove control or control enhancement from a control baseline		X
Change title of control or control enhancement	X	
Withdraw control or control enhancement not in a control baseline	X	
Withdraw control or control enhancement in a control baseline		X
Change a control or control enhancement not due to error (i.e., implementation is affected)		X
Change in discussion (e.g., reword for clarity, include examples)	X	
Significant change in discussion (e.g., change in intent)		X
Move control or control enhancement		X

SP 800-53A Revision 5 Assessment Procedure Schema: ODP- Selection

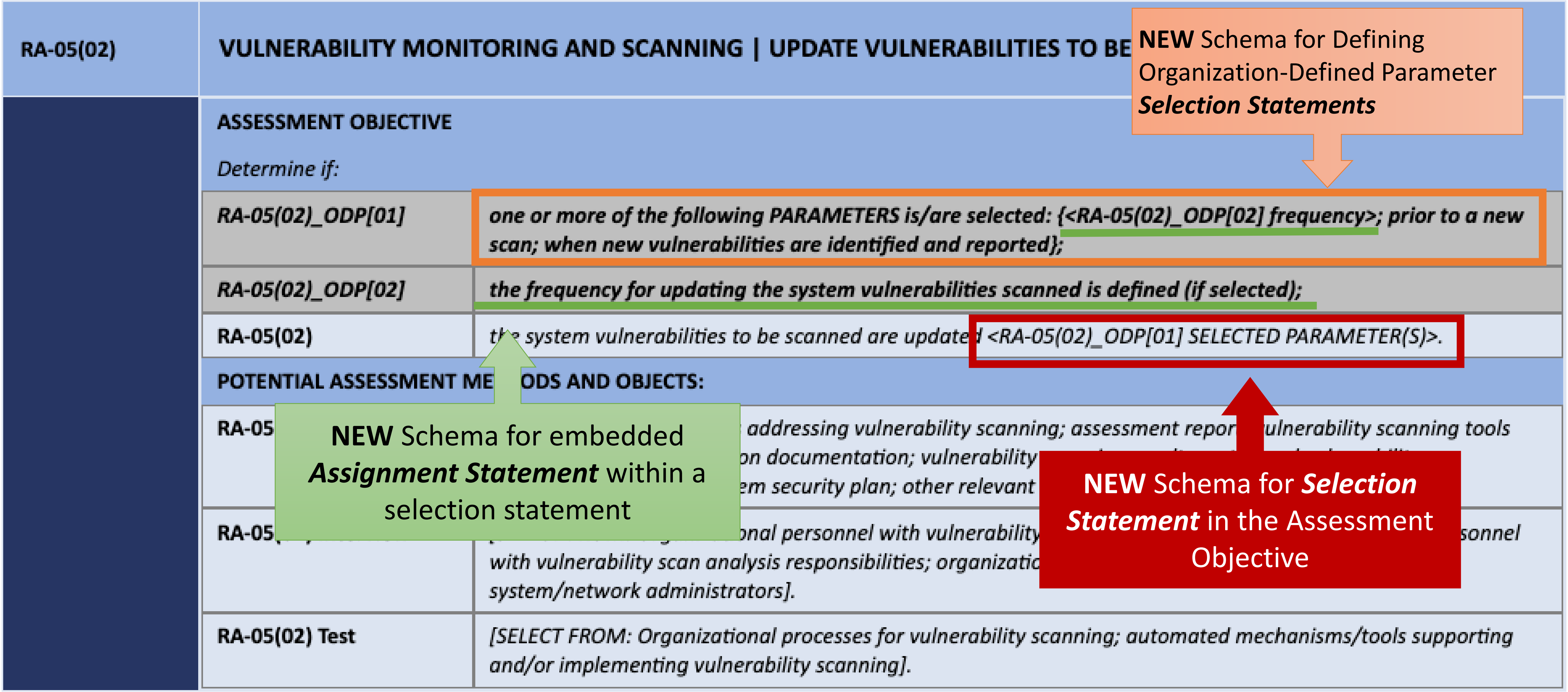
NEW Schema for Defining Organization-Defined Parameter ***Selection Statements***



AC-02(02)	ACCOUNT MANAGEMENT | AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT
	ASSESSMENT OBJECTIVE *Determine if:*
AC-02(02)_ODP[01]	***one of the following PARAMETERS is selected for automated management of temporary and emergency accounts: {remove; disable};***
AC-02(02)_ODP[02]	***the time period after which to automatically remove or disable temporary or emergency accounts is defined;***
AC-02(02)	*temporary and emergency accounts are automatically <AC-02(02)_ODP[01] SELECTED PARAMETER> after <AC-02(02)_ODP[02] time period>.*
	POTENTIAL ASSESSMENT METHODS AND OBJECTS:
AC-02(02) Examine	*[SELECT FROM: Access control policy; procedures fo system design documentation; system configuratio documentation; system-generated list of temporar system-generated list of emergency accounts remo records; system security plan; other relevant docur*
AC-02(02) Interview	*[SELECT FROM: Organizational personnel with account management responsibilities; system/network administrators; organizational personnel with information security with information security responsibilities; system developers].*
AC-02(02) Test	*[SELECT FROM: Automated mechanisms for implementing account management functions].*

ODP “unique ID” followed by SELECTED PARAMETER

SP 800-53A Revision 5 Assessment Procedure Schema: ODP- Assignment nested in Selection



RA-05(02)	VULNERABILITY MONITORING AND SCANNING | UPDATE VULNERABILITIES TO BE
	ASSESSMENT OBJECTIVE *Determine if:*
RA-05(02)_ODP[01]	***one or more of the following PARAMETERS is/are selected: {<RA-05(02)_ODP[02] frequency>; prior to a new scan; when new vulnerabilities are identified and reported};***
RA-05(02)_ODP[02]	***the frequency for updating the system vulnerabilities scanned is defined (if selected);***
RA-05(02)	*t e system vulnerabilities to be scanned are update <RA-05(02)_ODP[01] SELECTED PARAMETER(S)>.*
	POTENTIAL ASSESSMENT ME ODS AND OBJECTS:
RA-05	*addressing vulnerability scanning; assessment repor ulnerability scanning tools* *on documentation; vulnerability* *em security plan; other relevant*
RA-05	*onal personnel with vulnerability sonnel with vulnerability scan analysis responsibilities; organizatio system/network administrators].*
RA-05(02) Test	*[SELECT FROM: Organizational processes for vulnerability scanning; automated mechanisms/tools supporting and/or implementing vulnerability scanning].*

NEW Schema for Defining Organization-Defined Parameter ***Selection Statements***

NEW Schema for embedded ***Assignment Statement*** within a selection statement

NEW Schema for ***Selection Statement*** in the Assessment Objective