NIST 800-171 REV2 AND REV3

Crosswalk

Abstract

NIST SP 800-171 Revision 3 formally supersedes and withdraws Revision 2, aligning the requirements to the SP 800-53B moderate baseline through explicit tailoring and reorganizing them into 17 families. It adds new families—Planning (PL), System and Services Acquisition (SA), and Supply Chain Risk Management (SR)—while omitting Program Management (PM), PII Processing and Transparency (PT), and Contingency Planning (CP), except for the CP-09/09(08) backup-confidentiality exception; it also eliminates the “basic” vs. “derived” split, introduces organization-defined parameters (ODPs) for flexibility, tightens and titles requirement statements, groups related items, and removes redundant or outdated provisions while adding new ones to improve clarity and assessment readiness.

Arnold Villeneuve - AchievaTech.com

Arnold.Villeneuve@achievatech.com

Brief - Access Control (AC)

A crosswalk for the **Access Control (AC)** family between **NIST SP 800-171 Rev. 2** and **Rev. 3**. The table aligns each Rev. 2 requirement with its Rev. 3 counterpart and explains changes. A concise delta statement follows.

Evidence Table — AC Family Crosswalk (Rev. 2 → Rev. 3)

Rev 2 (ID – Title)	Rev 3 (ID – Title)	Explain the Difference
3.1.1 – Limit system access to authorized users, processes, and devices	**03.01.01 – Account Management**	Rev 3 expands account management: adds conditions to **disable** accounts (expired, inactive for an **ODP** time, disassociated, policy violation, **high-risk individuals**), adds **time-bound notifications** to account managers, and requires users to **log out after expected inactivity** (ODP) — with automatic enforcement covered by 03.01.10. NIST.SP.800-171r2 NIST.SP.800-171r3 NIST.SP.800-171r3 NIST.SP.800-171r3
3.1.2 – Limit access to types of transactions/functions	**03.01.02 – Access Enforcement**	Substantively aligned; Rev 3 explicitly says "enforce approved authorizations for **logical access to CUI and system resources**," clarifying scope. NIST.SP.800-171r2 NIST.SP.800-171r3
3.1.3 – Control the flow of CUI	**03.01.03 – Information Flow Enforcement**	Equivalent intent; Rev 3 discussion adds detail on **policy enforcement points** and **boundary devices**. NIST.SP.800-171r2

Rev 2 (ID – Title)	Rev 3 (ID – Title)	Explain the Difference
		NIST.SP.800-171r3
3.1.4 – Separation of duties	**03.01.04 – Separation of Duties**	Equivalent; Rev 3 reiterates that AC administrators should not administer **audit** functions and notes enforcement via 03.01.02. NIST.SP.800-171r2 NIST.SP.800-171r3
3.1.5 – Employ least privilege (incl. privileged accounts)	**03.01.05 – Least Privilege**	Same core requirement; Rev 3 adds an explicit **periodic review** of assigned privileges (ODP frequency) and enumerates examples of **security functions/security-relevant information**. NIST.SP.800-171r2 NIST.SP.800-171r3
3.1.6 – Use non-privileged accounts for non-security functions	**03.01.06 – Least Privilege – Privileged Accounts**	Rev 3 pulls privileged-account rules into a dedicated requirement and **requires** users with privileged accounts to use non-privileged accounts for non-security activities; also to **restrict** privileged accounts to defined roles. NIST.SP.800-171r2 NIST.SP.800-171r3
3.1.7 – Prevent non-privileged users from executing privileged functions; log such executions	**03.01.07 – Least Privilege – Privileged Functions**	Equivalent; Rev 3 preserves prohibition + logging and clarifies relationship to 03.01.01 and 03.01.02. NIST.SP.800-171r2 NIST.SP.800-171r3

Rev 2 (ID – Title)	Rev 3 (ID – Title)	Explain the Difference
3.1.8 – Limit unsuccessful logon attempts	**03.01.08 – Unsuccessful Logon Attempts**	Equivalent; Rev 3 enumerates possible **automated actions** (e.g., lock account/node for ODP period, delay prompt, notify admin) and retains the "delay algorithm" concept. NIST.SP.800-171r2 NIST.SP.800-171r3
3.1.9 – Provide privacy and security notices (system use notification)	**03.01.09 – System Use Notification**	Equivalent; Rev 3 wording compacted and tied to CUI context. NIST.SP.800-171r2 NIST.SP.800-171r3
3.1.10 – Use session lock with pattern-hiding displays	**03.01.10 – Device Lock**	Rev 3 renames to **Device Lock**, keeps pattern-hiding as an integrated element, and allows either **automatic** (ODP time) or **user-initiated** locking; explicitly states device locks don't replace logout. NIST.SP.800-171r2 NIST.SP.800-171r3
3.1.11 – Terminate a user session automatically after a defined condition	**03.01.11 – Session Termination**	Equivalent; Rev 3 keeps automatic termination triggered by **ODP conditions** and distinguishes from network disconnect (03.13.09). NIST.SP.800-171r2 NIST.SP.800-171r3
3.1.12 – Monitor and control remote access sessions	**03.01.12 – Remote Access**	Rev 3 **consolidates** remote-access management: usage restrictions, prior authorization, **route via managed access control points**, and **authorize privileged remote commands / access**

Rev 2 (ID – Title)	Rev 3 (ID – Title)	Explain the Difference
		to security-relevant info — absorbing Rev 2's 3.1.14 and 3.1.15. NIST.SP.800-171r3
3.1.13 – Use crypto to protect confidentiality of remote access sessions	**03.01.13 – Withdrawn; addressed by 03.13.08 (Transmission Confidentiality & Integrity)**	Rev 3 moves remote-session cryptography to **SC/03.13.08** in the System and Communications Protection family. NIST.SP.800-171r3 NIST.SP.800-171r3
3.1.14 – Route remote access via managed access control points	**03.01.12 – Remote Access; 03.01.14 – Withdrawn**	Functionality merged into **03.01.12(c)**; 03.01.14 is explicitly **withdrawn**. NIST.SP.800-171r3
3.1.15 – Authorize remote execution of privileged commands / access to security-relevant info	**03.01.12 – Remote Access; 03.01.15 – Withdrawn**	Functionality merged into **03.01.12(d)**; 03.01.15 is explicitly **withdrawn**. NIST.SP.800-171r3
3.1.16 – Authorize wireless access prior to connection	**03.01.16 – Wireless Access**	Equivalent with added specificity: Rev 3 adds **disable wireless networking when not intended for use** and keeps authentication/encryption. NIST.SP.800-171r3
3.1.17 – Protect wireless access using authentication and encryption	**03.01.16 – Wireless Access; 03.01.17 – Withdrawn**	Rev 3 consolidates under **03.01.16(d)** and marks 03.01.17 **withdrawn**. NIST.SP.800-171r3
3.1.18 – Control connection of mobile devices	**03.01.18 – Access Control for Mobile Devices**	Equivalent; Rev 3 packages usage/config/connection authorization and explicitly requires **full-device or**

Rev 2 (ID – Title)	Rev 3 (ID – Title)	Explain the Difference
		container-based encryption for CUI on mobile devices. NIST.SP.800-171r3 NIST.SP.800-171r3
3.1.19 – Encrypt CUI on mobile devices and mobile computing platforms	**03.01.18 – Access Control for Mobile Devices; 03.01.19 – Withdrawn**	Consolidated into **03.01.18(c)** (full-device or container-based encryption); 03.01.19 **withdrawn**. NIST.SP.800-171r3
3.1.20 – Verify and control/limit connections to and use of external systems	**03.01.20 – Use of External Systems**	Equivalent, with Rev 3: (a) allow **prohibition** unless specifically authorized, (b) require **ODP-defined** security requirements before use, (c) require verification/agreements, and (d) **restrict org-controlled portable storage** on external systems (absorbs 3.1.21). NIST.SP.800-171r2 NIST.SP.800-171r3
3.1.21 – Limit use of portable storage devices on external systems	**03.01.20 – Use of External Systems; 03.01.21 – Withdrawn**	Rev 3 incorporates portable-storage restrictions into **03.01.20(d)** and **withdraws** 03.01.21. NIST.SP.800-171r3
3.1.22 – Control CUI posted or processed on publicly accessible systems	**03.01.22 – Publicly Accessible Content**	Equivalent intent (training + review/removal if discovered), streamlined wording. NIST.SP.800-171r2 NIST.SP.800-171r3

Sources for Rev. 2 AC requirements and mappings: Ch. 3 §3.1 & Appendix D Tables (e.g., D-1) in Rev. 2.

NIST.SP.800-171r2

NIST.SP.800-171r2

Sources for Rev. 3 AC requirements, withdrawals & tailoring: §3.1 and Appendix C Table 3, plus ODPs in Appendix D.

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

Delta Statement — What's New/Different in Rev. 3 (AC Family)

- **Consolidation of Remote Access.** Rev 3 merges Rev 2's 3.1.12, 3.1.14, and 3.1.15 into a single **03.01.12 Remote Access** requirement (monitor/authorize, route via managed access control points, and authorize privileged remote commands). The old 03.01.14 and 03.01.15 entries are **withdrawn**.

NIST.SP.800-171r3

- **Cryptography for Remote Sessions relocated.** Rev 2's 3.1.13 becomes **03.01.13 Withdrawn**; confidentiality/integrity protection is addressed in **03.13.08** (SC family).

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Wireless Access tightened.** Rev 3 adds an explicit control to **disable wireless networking when not intended for use** (03.01.16(c)) and withdraws 03.01.17 (consolidated into 03.01.16).

NIST.SP.800-171r3

- **Mobile Device encryption unified.** Rev 2's separate encryption requirement (3.1.19) is rolled into **03.01.18(c)**; 03.01.19 is **withdrawn**.

NIST.SP.800-171r3

- **External Systems integrated.** Rev 2's 3.1.21 is absorbed into **03.01.20(d)** (restrict org-controlled portable storage on external systems); 03.01.21 is **withdrawn**.

NIST.SP.800-171r3

- **Device Lock terminology and options. Session Lock** becomes **03.01.10 Device Lock**, still requiring pattern-hiding displays but explicitly allowing **automatic** (ODP time) or **user-initiated** locking.

NIST.SP.800-171r3

- **Least Privilege sharpened.** Rev 3 adds an explicit **privilege review cadence** (ODP) in **03.01.05**, separates **privileged accounts** into **03.01.06**, and keeps logging/prohibition of privileged functions in **03.01.07**.

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Account management specificity. 03.01.01** adds actionable conditions (e.g., **disable high-risk individuals**, **inactivity logout**, **manager notifications** with ODP timeframes).

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Structural changes across Rev. 3.** Rev 3 **eliminates the basic/derived split**, **adds titles**, introduces **organization-defined parameters (ODPs)** for flexibility, and groups/removes requirements to streamline assessments. (Affects AC and the rest of Sec. 3.)

NIST.SP.800-171r3

Conflicts

- **AC-17 mapping ambiguity.** Appendix C Table 3 shows AC-17 mapping partly to **03.01.02** and to **03.01.12**/**03.13.08**; the requirement text clearly concentrates remote-access management in **03.01.12**, with crypto moved to **03.13.08**. Use the requirement text as the authoritative crosswalk for implementation.

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

Gaps

- **ODP values needed.** Rev. 3 adds ODPs for **timeouts**, **notification windows**, **review frequencies**, and **security requirements for external systems**. These require organization-specific values to complete implementation.

NIST.SP.800-171r3

- **Policy updates.** Consolidations/withdrawals (e.g., remote access, wireless, mobile, external systems) require rewriting existing policy sections that referenced the old 3.1.13–3.1.21 structure.

NIST.SP.800-171r3

NIST.SP.800-171r3

Recommendations

1. **Set ODPs for AC:** Define and document timeouts (device lock, inactivity logout), failed-login thresholds/actions, privilege review frequency, and security requirements for external systems. Tie them into SSP and procedures.

NIST.SP.800-171r3

2. **Revise remote access policy:** Collapse prior 3.1.12/14/15 into a single **Remote Access** section aligned to **03.01.12**; ensure crypto requirements are referenced from **03.13.08**.

NIST.SP.800-171r3

NIST.SP.800-171r3

3. **Update wireless and mobile standards:** Add "**disable when not in use**" for wireless; require **full-device or container encryption** for CUI on mobile devices.

NIST.SP.800-171r3

NIST.SP.800-171r3

4. **Harden privileged access operations:** Break out privileged account governance (03.01.06) and maintain logs of privileged functions (03.01.07).

NIST.SP.800-171r3

5. **Re-baseline external system usage:** Fold portable-storage restrictions into **03.01.20** controls and set pre-use security requirements and agreement templates.

NIST.SP.800-171r3

Brief - Awareness & Training (AT)

Awareness & Training (AT) in Rev 3 consolidates and modernizes Rev 2's three AT requirements. Rev 3 renames "awareness" to **security literacy**, pulls the Rev 2 insider-threat requirement into the main literacy requirement, adds explicit coverage of **social engineering and social mining**, and introduces **organization-defined parameters (ODPs)** for training frequency and update triggers. Role-based training remains, but with clearer timing gates ("before authorizing access" and on defined events).

NIST.SP.800-171r3

NIST.SP.800-171r3

Evidence Table (Crosswalk — Awareness & Training)

Rev 2 Column	Rev 3 Column	Explain the Difference
3.2.1 — Ensure managers, admins, and users are made aware of security risks and applicable policies, standards, and procedures. (AT awareness) NIST.SP.800-171r2	**03.02.01 Literacy Training and Awareness** — Provide security **literacy** training: (1) as part of initial training and at an **[org-defined frequency]** thereafter; (2) when required by **system changes** or following **[org-defined events]**; (3) include recognizing and reporting **insider threat, social engineering, and social mining**. Also **update** training content at an **[org-defined frequency]** and after **[org-defined events]**. NIST.SP.800-171r3 NIST.SP.800-171r3	Rev 3 reframes "awareness" as **literacy**, **adds ODPs** for cadence/triggers, and **expands content** to include social engineering and social mining in addition to insider-threat awareness. It also introduces an explicit requirement to **update** content on a defined schedule or events. Table 4 confirms AT-02(02) and AT-02(03) map into 03.02.01. NIST.SP.800-171r3

Rev 2 Column	Rev 3 Column	Explain the Difference
3.2.2 — Ensure personnel are trained to carry out assigned information-security duties and responsibilities (role-based). NIST.SP.800-171r2 NIST.SP.800-171r2	**03.02.02 Role-Based Training** — Provide role-based training **before** authorizing access to the system or CUI, **before** performing assigned duties, and at an **[org-defined frequency]** thereafter; also when required by **system changes** or following **[org-defined events]**. **Update** role-based content at an **[org-defined frequency]** and after **[org-defined events]**. NIST.SP.800-171r3	Core concept is retained, but Rev 3 adds explicit **timing gates** (before access/before duties), introduces **ODPs** for cadence/triggers, and requires **content updates** on defined schedules or events. NIST.SP.800-171r3
3.2.3 (Derived) — Provide awareness training on recognizing and reporting potential **insider-threat** indicators. NIST.SP.800-171r2	**03.02.03 — Withdrawn**; **incorporated into 03.02.01** (literacy training). NIST.SP.800-171r3	Rev 3 **folds** the separate insider-threat requirement into 03.02.01 and, at the same time, **broadens** it to include **social engineering** and **social mining** topics. Table 4 shows the AT-02(02) and new AT-02(03) elements aligning with 03.02.01. NIST.SP.800-171r3

Additional reference points

- Rev 3's **Table 4 (Awareness and Training)** maps SP 800-53 controls to Rev 3 requirements, showing **AT-02(02) Insider Threat** and **AT-02(03) Social Engineering and Mining** both tailored to **03.02.01**, and **AT-03** to **03.02.02**. (See p. 95).

NIST.SP.800-171r3

- Rev 2's Appendix E shows the AT tailoring actions from 800-53 (AT-1/AT-4 NFO, AT-2/AT-3 CUI), consistent with the three Rev 2 AT requirements.

NIST.SP.800-171r2

Conflicts

- **Numbering and naming**: Rev 2 uses 3.2.x “Awareness and Training”; Rev 3 uses **03.02.xx “Literacy Training and Awareness / Role-Based Training”**. This is a terminology/structure change, not a reduction in scope.

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Location of insider-threat content**: In Rev 2 it is a **separate derived** requirement (3.2.3); in Rev 3 it is **integrated** within 03.02.01 along with new topics (social engineering/mining). Some legacy mappings that expect a one-to-one control may appear “missing” unless the consolidation is recognized.

NIST.SP.800-171r2

NIST.SP.800-171r3

Gaps

- **ODP values not set**: Rev 3 requires organizations (or their agencies) to **assign values** for training **frequency** and **event-based triggers** for both 03.02.01 and 03.02.02; these are not specified by NIST and must be defined locally.

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Expanded content coverage**: Existing curricula may lack **social engineering** and **social mining** content now called out explicitly in 03.02.01.

NIST.SP.800-171r3

- **Content update requirement**: Rev 3 adds normative language to **update** training content at [org-defined] intervals and after [org-defined] events. Programs that only deliver annual training without updates after incidents or system changes will not meet the letter of Rev 3.

NIST.SP.800-171r3

NIST.SP.800-171r3

Recommendations

1. **Set ODPs**: Document organization-defined **frequency** (e.g., onboarding + at least annually) and **event triggers** (e.g., major system change, significant incident, audit findings) for both literacy and role-based training; include the cadence for **content updates**.

NIST.SP.800-171r3

NIST.SP.800-171r3

2. **Update curricula**: Incorporate modules on **insider-threat indicators**, **social engineering** (phishing, pretexting, impersonation, baiting, quid pro quo, threadjacking, social-media exploitation, tailgating), and **social mining**, with clear **reporting channels**.

NIST.SP.800-171r3

3. **Gate access with training**: Enforce role-based training **prior to** granting system or CUI access and **before** personnel assume security-relevant duties; record the gating in access workflows.

NIST.SP.800-171r3

4. **Keep records anyway**: Although training-records control (AT-04) is **NCO/out of scope** in Rev 3, retain auditable records to support assessments and external attestations. (See Table 4 noting AT-04=NCO).

NIST.SP.800-171r3

5. **Map legacy 3.2.3 to 03.02.01**: Update internal crosswalks/checklists so teams don't falsely mark insider-threat training as "missing" in Rev 3.

NIST.SP.800-171r3

Delta Statement (What's new/different in Rev 3 — AT)

- **Consolidation**: Rev 2's separate **3.2.3 (Insider Threat)** is **withdrawn and merged** into **03.02.01**, which now serves as the single literacy/awareness requirement.

NIST.SP.800-171r3

- **Expanded scope**: Literacy training now explicitly includes **social engineering and social mining** topics beyond insider threats. (Table 4 shows AT-02(03) mapping to 03.02.01.)

NIST.SP.800-171r3

- **ODPs introduced**: Rev 3 requires organizations to **define frequency and event-based triggers** for delivering and updating both literacy and role-based training; these parameters must be set locally.

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Timing gates clarified**: Role-based training must occur **before authorizing access** to systems/CUI and **before** performing assigned duties, not just "as needed."

NIST.SP.800-171r3

Brief - Audit & Accountability (AU)

Below is a verified crosswalk for **Audit & Accountability (AU)** between **NIST SP 800-171 Rev. 2 (Rev 2)** and **Rev. 3 (Rev 3)**. I aligned every AU security requirement in Rev 2 (3.3.1–3.3.9) to its Rev 3 counterpart (03.03.01–03.03.09) and noted notable AU-related SP 800-53 control tailoring differences visible in each revision's AU tables. I validated the set and wording from **Rev 2 Appendix D, Table D-3 (pp. 66–68)** and **Rev 2 Appendix E, Table E-3 (pp. 87–88)** against the **Rev 3 AU table (Table 5, p. 95)** and the **Rev 3 main text for 03.03.01–03.03.09 (pp. 22–27)**.

NIST.SP.800-171r2

NIST.SP.800-171r2

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

Evidence Table — AU Crosswalk (Rev 2 ↔ Rev 3)

Rev 2 (3.3.x)	**Rev 3 (03.03.xx)**	**Explain the difference**
3.3.1 Create and retain system audit logs and records to enable monitoring/analysis/investigation/reporting. NIST.SP.800-171r2	**03.03.01** Event Logging (select, review, and update event types) **and 03.03.03** Audit Record Generation (generate records; retain per policy). NIST.SP.800-171r3	Rev 3 separates "what to log" (selection & periodic review) from "generate and retain," adds explicit **organization-defined review**

Rev 2 (3.3.x)	Rev 3 (03.03.xx)	Explain the difference
	NIST.SP.800-171r3	**frequency** and **retention tied to records policy**. NIST.SP.800-171r3 NIST.SP.800-171r3
3.3.2 Ensure actions of individual users can be uniquely traced to those users. NIST.SP.800-171r2	**03.03.02** Audit Record Content (must include identity of individuals/subjects/objects/entities for events). NIST.SP.800-171r3	Rev 3 embeds traceability as required **audit content** (identity fields and outcomes), rather than a standalone requirement. NIST.SP.800-171r3
3.3.3 Review and update logged events. NIST.SP.800-171r2	**03.03.01(b)** Review and update the **event types** selected for logging at an organization-defined frequency. NIST.SP.800-171r3	Same intent; Rev 3 makes it an explicit sub-requirement of Event Logging and requires a defined cadence. NIST.SP.800-171r3
3.3.4 Alert on audit logging process failure. NIST.SP.800-171r2	**03.03.04** Response to Audit Logging Process Failures (alert within org-defined time; define additional actions). NIST.SP.800-171r3	Rev 3 expands with **time-to-alert** and **org-defined response actions** (e.g., overwrite oldest logs, stop generation). NIST.SP.800-171r3

Rev 2 (3.3.x)	Rev 3 (03.03.xx)	Explain the difference
3.3.5 Correlate audit record review/analysis/reporting across repositories. NIST.SP.800-171r2	**03.03.05(c)** Analyze and **correlate across repositories** for organization-wide awareness. NIST.SP.800-171r3	Same capability, now integrated into the broader review/analysis/reporting requirement with added context/examples. NIST.SP.800-171r3
3.3.6 Provide audit record reduction and report generation to support on-demand analysis. NIST.SP.800-171r2	**03.03.06** Audit Record Reduction and Report Generation (and **preserve original content and time ordering**). NIST.SP.800-171r3	Rev 3 adds an explicit requirement to **preserve original content and ordering** when reducing/generating reports. NIST.SP.800-171r3
3.3.7 Compare and **synchronize** internal system clocks with an authoritative source to generate timestamps. NIST.SP.800-171r2	**03.03.07** Time Stamps (use internal clocks; record timestamps with org-defined granularity; use **UTC or include local offset**). NIST.SP.800-171r3	Rev 3 focuses on **granularity** and **UTC/offset**; it does **not** explicitly require synchronization with an external authoritative source as Rev 2 did. NIST.SP.800-171r3
3.3.8 Protect audit information and tools from unauthorized access/modification/deletion. NIST.SP.800-171r2	**03.03.08(a)** Protect audit information and logging tools **and 03.03.08(b)** restrict management of logging to a subset of privileged users/roles.	Rev 3 **adds** the management-restriction clause directly in 03.03.08(b), consolidating

Rev 2 (3.3.x)	Rev 3 (03.03.xx)	Explain the difference
	NIST.SP.800-171r3	Rev 2's 3.3.8 and 3.3.9. NIST.SP.800-171r3
3.3.9 Limit management of audit logging to a subset of privileged users. NIST.SP.800-171r2	**03.03.09 Withdrawn — incorporated into 03.03.08**. NIST.SP.800-171r3	Rev 3 eliminates the separate requirement and embeds it as 03.03.08(b). NIST.SP.800-171r3

Tailoring / SP 800-53 control notes for completeness (both revisions' AU tables):

- **AU-04 Audit Log Storage Capacity** remains **NCO** (not tied to a 171 security requirement) in both revisions' AU tables. Rev 3 keeps it with no mapped 03.03.x requirement.

NIST.SP.800-171r2

NIST.SP.800-171r3

- **AU-06(01)** and **AU-07(01)** remain **NCO** options in both revisions.

NIST.SP.800-171r2

NIST.SP.800-171r3

- **AU-08(01) Time Synchronization** was tailored **in Rev 2**; Rev 3's AU table lists only **AU-08** (no (01)), while 03.03.07 covers **UTC/offset and granularity** instead of explicit authoritative synchronization.

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Retention emphasis:** In Rev 2, **AU-11** (retention) appears as **NCO** in tailoring, even though 3.3.1 mentions "retain." Rev 3 upgrades retention into core AU by placing **AU-11 and AU-12** under **03.03.03** (**CUI**), explicitly requiring retention per policy.

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

Conflicts

- **Time synchronization vs. timestamp granularity:** Rev 2 explicitly required **synchronization with an authoritative source** (3.3.7). Rev 3 (03.03.07) emphasizes **UTC/offset and granularity** but **does not state** authoritative synchronization. If you previously documented a specific external time source, that citation is not mandated by Rev 3 language.

NIST.SP.800-171r2

NIST.SP.800-171r3

- **Retention placement:** Teams may read Rev 2 as already requiring retention via 3.3.1; however, Rev 2's AU-11 was tailored **NCO**, while Rev 3 makes retention explicit in **03.03.03** (CUI). Treat as a **strengthening/clarification** rather than a net-new domain.

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

Gaps (organization-defined parameters that must be set under Rev 3)

- **Event types & review cadence** for logging (**03.03.01(b)**).

NIST.SP.800-171r3

- **Alert time window** and **additional actions** for logging process failures (**03.03.04**).

NIST.SP.800-171r3

- **Timestamp granularity** and **UTC/offset approach** for all audit records (**03.03.07**).

NIST.SP.800-171r3

- **Audit record retention period** aligned to your records policy (**03.03.03(b)**).

NIST.SP.800-171r3

Recommendations

1. **Update AU policies & procedures** to reflect Rev 3 structure—especially the roll-up of management restrictions into **03.03.08(b)** and the explicit retention requirement in **03.03.03**. Cross-reference the family-level policy pointer (**AU-01 → 03.15.01**) in your master policy index.

NIST.SP.800-171r3

NIST.SP.800-171r3

2. **Tune your SIEM/logging platform** to (a) document selected event types; (b) schedule a review/update frequency; and (c) preserve original content and time ordering in reports.

NIST.SP.800-171r3

NIST.SP.800-171r3

3. **Define alert SLAs and playbooks** for audit logging failures, including storage-capacity responses.

NIST.SP.800-171r3

4. **Set timestamp standards** (UTC or local+offset) and minimum granularity across all systems; decide whether to **retain external time-source synchronization** as a best practice even though Rev 3 does not require it explicitly.

NIST.SP.800-171r3

5. **Document retention periods** in your records schedule and confirm your log storage architecture supports the required duration and integrity.

NIST.SP.800-171r3

Delta Statement — What's new/different in Rev 3 (AU)

- **Restructured & clearer requirements:** Logging selection/review (**03.03.01**) and generation/retention (**03.03.03**) are separated and more prescriptive (review **frequency**, **retention per policy**).

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Consolidation:** Management restriction on audit logging moved into **03.03.08(b)**; **03.03.09 is withdrawn**.

NIST.SP.800-171r3

- **Strengthened failure response:** Requires **time-to-alert** and **defined actions** for logging process failures.

NIST.SP.800-171r3

- **Timestamp modernization:** Focus on **UTC/offset** and **granularity**; the explicit authoritative time-source sync from Rev 2 is not restated.

NIST.SP.800-171r3

- **Tailoring changes surfaced: AU-11** (retention) now clearly part of core AU via **03.03.03 (CUI)** in Rev 3 AU table, whereas Rev 2 listed AU-11 as **NCO** in tailoring.

NIST.SP.800-171r3

NIST.SP.800-171r2

Brief

Below is a crosswalk for the **Audit and Accountability (AU)** family, aligning **NIST SP 800-171 Rev. 2 §3.3.x** with **NIST SP 800-171 Rev. 3 §03.03.xx** and explaining deltas. **Verification:** Rev. 2 contains nine AU requirements (**3.3.1–3.3.9**). Rev. 3 contains eight active AU requirements (**03.03.01–03.03.08**) and marks **03.03.09** as *withdrawn* and incorporated into **03.03.08**. All AU controls from both revisions are included below.

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

Evidence Table (Rev-to-Rev Crosswalk — Audit & Accountability)

Rev 2 (number & title)	Rev 3 (number & title)	Explain the difference
3.3.1 Create and retain system audit logs and records to enable monitoring, analysis, investigation, and reporting. NIST.SP.800-171r2	**03.03.01 Event Logging**; **03.03.02 Audit Record Content**; **03.03.03 Audit Record Generation**; **03.03.05 Audit Record Review, Analysis, and Reporting** NIST.SP.800-171r3 NIST.SP.800-171r3 NIST.SP.800-171r3 NIST.SP.800-171r3	Rev. 3 decomposes Rev. 2's broad requirement into: selecting/reviewing logged **event types** (03.03.01), specifying **audit content** (03.03.02), **generating and retaining** audit records (03.03.03 explicitly includes retention), and the **review/analysis/reporting** activity (03.03.05). Functional intent is preserved but made more granular and assessment-friendly. NIST.SP.800-171r3 NIST.SP.800-171r3
3.3.2 Ensure actions of individual users can be uniquely traced to those users.	**03.03.02 Audit Record Content** (includes identity of subjects/objects/entities) and **03.03.03 Audit Record Generation** (ensure	Rev. 3 achieves traceability by mandating specific **content fields** (e.g., identity, time, source, outcome) rather than a standalone traceability

Rev 2 (number & title)	Rev 3 (number & title)	Explain the difference
NIST.SP.800-171r2	generation/retention of records) NIST.SP.800-171r3 NIST.SP.800-171r3	statement. Outcome: same objective, clearer test points. NIST.SP.800-171r3
3.3.3 Review and update logged events. NIST.SP.800-171r2	**03.03.01 Event Logging** (03.03.01.b requires periodic review/update of selected event types; ODP for frequency) NIST.SP.800-171r3 NIST.SP.800-171r3	Substantively equivalent; Rev. 3 adds **organization-defined parameter (ODP)** for review frequency, making cadence explicit. NIST.SP.800-171r3
3.3.4 Alert in the event of an audit logging process failure. NIST.SP.800-171r2	**03.03.04 Response to Audit Logging Process Failures** (requires alert **within an ODP-defined time** and to take **ODP-defined additional actions**) NIST.SP.800-171r3 NIST.SP.800-171r3	Rev. 3 expands Rev. 2 by adding **timeliness** and **explicit response actions** parameters and clarifies scope (repository, system, or enterprise capacity). NIST.SP.800-171r3
3.3.5 Correlate audit record review, analysis, and reporting processes... NIST.SP.800-171r2	**03.03.05 Audit Record Review, Analysis, and Reporting** (includes correlation across repositories for org-wide situational awareness) NIST.SP.800-171r3	Intent carried forward; Rev. 3 spells out **correlation across repositories** and reporting to designated roles; adds ODP for review frequency. NIST.SP.800-171r3 NIST.SP.800-171r3
3.3.6 Provide audit record reduction and report generation.	**03.03.06 Audit Record Reduction and Report Generation** (preserve	Equivalent control with added emphasis on preserving **original**

Rev 2 (number & title)	Rev 3 (number & title)	Explain the difference
NIST.SP.800-171r2	original content and time ordering) NIST.SP.800-171r3	**content/time order**; discussion aligns closely with Rev. 2. NIST.SP.800-171r3
3.3.7 Provide capability to compare/synchronize internal clocks with an authoritative source to generate time stamps. NIST.SP.800-171r2	**03.03.07 Time Stamps** (use internal clocks; record UTC or fixed offset; **ODP-defined granularity**) NIST.SP.800-171r3 NIST.SP.800-171r3	Equivalent objective; Rev. 3 adds explicit **granularity** parameter and permitted time representations (UTC/offset). NIST.SP.800-171r3
3.3.8 Protect audit information and tools from unauthorized access, modification, deletion. NIST.SP.800-171r2	**03.03.08 Protection of Audit Information** (part a) NIST.SP.800-171r3	Substantively equivalent; Rev. 3 carries forward scope and clarifies technical vs. physical protections. NIST.SP.800-171r3
3.3.9 Limit management of audit logging functionality to a subset of privileged users. NIST.SP.800-171r2	**03.03.08 Protection of Audit Information** (part b); **03.03.09 Withdrawn — incorporated into 03.03.08** NIST.SP.800-171r3	Rev. 3 **merges** this explicit limitation into **03.03.08(b)** and declares **03.03.09 withdrawn**. Net effect: no loss of requirement; structurally consolidated. NIST.SP.800-171r3

Supplementary alignment (normative table view): Rev. 3's **Table 5** confirms the AU-to-requirement mapping (e.g., AU-02→03.03.01; AU-03→03.03.02; AU-11/12→03.03.03; AU-05→03.03.04; AU-06/-06(03)→03.03.05; AU-07→03.03.06; AU-08→03.03.07; AU-09/-09(04)→03.03.08).

NIST.SP.800-171r3

Conflicts

- **Numbering vs. scope ambiguity (3.3.1 ↔ multiple 03.03.xx):** Rev. 2 bundled *creation, content, retention, and analysis* into 3.3.1; Rev. 3 splits these across four distinct requirements (03.03.01, .02, .03, .05). This is a structural change, not a substantive reduction.

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Privilege limitation location:** Rev. 2 had a dedicated 3.3.9; Rev. 3 integrates it into **03.03.08(b)** and marks **03.03.09** withdrawn—teams might mistakenly think the privilege limitation was removed; it was **not**.

NIST.SP.800-171r3

Gaps

- **ODP values required in Rev. 3:** Frequency for event-type reviews (**03.03.01**), alert time and actions for logging failures (**03.03.04**), review frequency (**03.03.05**), and timestamp granularity (**03.03.07**) must be **defined by the organization or customer**; these values are not specified by NIST.

NIST.SP.800-171r3

- **Policy & procedures scoping:** AU policy & procedures map to the common requirement **03.15.01** rather than a family-specific AU identifier; ensure your governance documents reflect this cross-family treatment.

NIST.SP.800-171r3

Recommendations

1. **Update control narratives to Rev. 3 structure.** Split your Rev. 2 3.3.1 narrative into: *Event Selection/Review (03.03.01), Record Content (03.03.02), Generation & Retention (03.03.03), and Review/Analysis/Reporting (03.03.05).* This makes assessments clearer and aligns to 171A Rev. 3.

NIST.SP.800-171r3

NIST.SP.800-171r3

2. **Define ODPs and embed in procedures:**
    - Event-type review cadence (03.03.01.b)
    - Alert time and additional actions for logging failures (03.03.04.a–b)
    - Audit review frequency (03.03.05.a)
    - Time-stamp granularity and UTC/offset choice (03.03.07.b)

NIST.SP.800-171r3

3. **Document the consolidation of privileges:** Fold Rev. 2's 3.3.9 into your **03.03.08(b)** procedure so access to audit-logging management remains restricted to an approved subset of privileged roles. Cite the withdrawal note for 03.03.09 to avoid audit confusion.

NIST.SP.800-171r3

4. **Re-validate SIEM/SOAR configurations:** Confirm that your tooling captures **all Rev. 3 content elements** and supports correlation across repositories as explicitly required in **03.03.05(c)**.

NIST.SP.800-171r3

5. **Retain evidence mapping:** Keep a trace matrix that links each Rev. 2 AU control to its Rev. 3 successor(s) per the table above and **Rev. 3 Table 5** for auditor transparency.

NIST.SP.800-171r3

Delta Statement (What's new/different in Rev. 3 — AU)

- **Structural refactor:** Rev. 2's broad **3.3.1** is **split** across **03.03.01, 03.03.02, 03.03.03, and 03.03.05**, making selection, content, generation/retention, and analysis explicit.

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Consolidation:** Rev. 2 **3.3.9** is **merged** into **03.03.08(b)**; **03.03.09 is withdrawn** (no requirement loss).

NIST.SP.800-171r3

- **Parameterized expectations:** Rev. 3 introduces **organization-defined parameters** for alert timing, review cadence, and timestamp granularity, which were implicit or absent in Rev. 2.

NIST.SP.800-171r3

- **Clarified semantics:** Rev. 3 emphasizes correlation **across repositories** and preserving **original content/time order** during reduction/reporting; it also clarifies allowable timestamp standards (UTC/offset).

NIST.SP.800-171r3

NIST.SP.800-171r3

Brief — Configuration Management (CM) Crosswalk (NIST SP 800-171 Rev.2 → Rev.3)
Below is a complete, control-by-control alignment of CM requirements from Rev.2 (3.4.x) to Rev.3 (03.04.xx). Every CM requirement from both revisions is included. Headline deltas: Rev.3 splits "baseline + inventory" into two separate requirements; folds Rev.2's "restrict nonessential ports/protocols/services" into Least Functionality and Authorized Software; removes the dedicated "user-installed software" control (managed via AC/CA and allow-lists); and adds two new requirements—Information Location and High-Risk Area configurations. Coverage verified against Rev.3 Table 7 and Rev.3 §3.4 text.

NIST.SP.800-171r3

NIST.SP.800-171r3

Evidence Table — CM Family Crosswalk (Rev.2 ↔ Rev.3)

Rev 2 (3.4.x)	**Rev 3 (03.04.xx)**	**Explain the Difference**
3.4.1 Baseline configurations and inventories. Establish & maintain baseline configs **and** inventories throughout the SDLC. NIST.SP.800-171r2	**03.04.01 Baseline Configuration and 03.04.10 System Component Inventory**. Baseline under configuration control with periodic review; inventory is its own requirement with update triggers. NIST.SP.800-171r3 NIST.SP.800-171r3	Rev.3 **splits** Rev.2's combined requirement into two: baseline (03.04.01) and inventory (03.04.10). Inventory now has explicit review/update cadence and event-driven updates. NIST.SP.800-171r3 NIST.SP.800-171r3

Rev 2 (3.4.x)	Rev 3 (03.04.xx)	Explain the Difference
3.4.2 Security configuration settings. Establish/enforce secure settings for IT products. NIST.SP.800-171r2	**03.04.02 Configuration Settings**. Establish settings in "most restrictive mode," approve deviations; settings become part of baseline. NIST.SP.800-171r3	Substantively aligned; Rev.3 adds explicit "**most restrictive mode**" language and keeps settings as part of the configuration baseline. NIST.SP.800-171r3
3.4.3 Configuration change control. Track/review/approve-or-disapprove & log changes. NIST.SP.800-171r2	**03.04.03 Configuration Change Control**. Defines what's configuration-controlled; requires review with security impact; monitor activities. NIST.SP.800-171r3	Same intent; Rev.3 enumerates steps (a–d) and clarifies scope (baseline, settings, unauthorized changes, vulnerability remediation). NIST.SP.800-171r3
3.4.4 Analyze security impact of changes prior to implementation. NIST.SP.800-171r2	**03.04.04 Impact Analyses**. Analyze **before** changes **and verify** controls **after** changes; notes supply-chain impacts. NIST.SP.800-171r3	Rev.3 adds a **post-change verification** step and expands discussion;

Rev 2 (3.4.x)	Rev 3 (03.04.xx)	Explain the Difference
		otherwise aligned. NIST.SP.800-171r3
3.4.5 Access restrictions for change (define, document, approve, enforce). NIST.SP.800-171r2	**03.04.05 Access Restrictions for Change**. Same focus; includes examples (software/media libraries, change windows). NIST.SP.800-171r3	Substantively aligned; Rev.3 adds detail, retains physical & logical restriction emphasis. NIST.SP.800-171r3
3.4.6 Least functionality (provide only essential capabilities). NIST.SP.800-171r2	**03.04.06 Least Functionality**. Add explicit prohibition/restriction list (functions/ports/protocols/connections/ services), **periodic review** (ODP), and disable/remove actions. NIST.SP.800-171r3	Rev.3 **strengthens** least functionality with ODP review cadence and explicit port/protocol/service controls—partly absorbing Rev.2 3.4.7. NIST.SP.800-171r3
3.4.7 Restrict/disable/prevent nonessential programs, functions, ports, protocols, services.	**03.04.06** (Least Functionality) **and 03.04.08** (Authorized Software – Allow by Exception); **03.04.07 is withdrawn**. NIST.SP.800-171r3	Rev.3 **removes** a stand-alone requirement and **integrates** it into least

Rev 2 (3.4.x)	Rev 3 (03.04.xx)	Explain the Difference
NIST.SP.800-171r2		functionality plus allow-listed software control. NIST.SP.800-171r3
3.4.8 Blacklist or whitelist software (deny-by-exception or deny-all/allow-by-exception). NIST.SP.800-171r2	**03.04.08 Authorized Software – Allow by Exception** only; maintain allow-list and review it periodically (ODP). NIST.SP.800-171r3	Rev.3 **drops blacklisting** as an option—**mandates allow-listing** (deny-all, allow-by-exception). Stronger control posture. NIST.SP.800-171r3
3.4.9 Control and monitor user-installed software. NIST.SP.800-171r2	**03.04.09 Withdrawn**—addressed by AC least-privilege/separation-of-duties, allow-listed software, and continuous monitoring (**03.01.05/06/07**, **03.04.08**, **03.12.03**). NIST.SP.800-171r3	Rev.3 **removes** the dedicated CM control; management of user installs is enforced via AC/CA families and allow-lists. NIST.SP.800-171r3 NIST.SP.800-171r3
—	**03.04.07 Withdrawn** (incorporated into 03.04.06 & 03.04.08).	Included here for completeness of the Rev.3 list;

Rev 2 (3.4.x)	Rev 3 (03.04.xx)	Explain the Difference
	NIST.SP.800-171r3	content covered elsewhere in CM. NIST.SP.800-171r3
—	**03.04.11 Information Location**. Identify/document **where CUI resides** and the components that process/store it; document changes. NIST.SP.800-171r3	**New in Rev.3**; no Rev.2 counterpart—adds explicit accountability for **CUI location** across components. NIST.SP.800-171r3
—	**03.04.12 System & Component Configuration for High-Risk Areas** (e.g., travel laptops; pre/post controls). NIST.SP.800-171r3	**New in Rev.3**; elevates CM-2(07) concept—Rev.2 treated this enhancement as out-of-scope (NFO) for 800-171; Rev.3 makes it a CUI requirement. NIST.SP.800-171r2 NIST.SP.800-171r3

Delta Statement (CM Family — What's new/different in Rev.3)

1. **Split of 3.4.1**: Rev.2's combined "baseline + inventory" becomes **03.04.01 Baseline Configuration** and **03.04.10 System Component Inventory**, each with explicit review/update triggers.

NIST.SP.800-171r3

NIST.SP.800-171r3

2. **Least Functionality strengthened**: **03.04.06** adds ODP-driven periodic review, explicit prohibit/restrict lists for ports/protocols/connections/services, and folds in the Rev.2 3.4.7 concepts; **03.04.07** is withdrawn accordingly.

NIST.SP.800-171r3

3. **Allow-listing required**: **03.04.08** mandates a **deny-all, allow-by-exception** policy; Rev.2 allowed blacklisting or whitelisting under 3.4.8.

NIST.SP.800-171r2

NIST.SP.800-171r3

4. **User-installed software control retired from CM**: Rev.2 **3.4.9** is **withdrawn** in Rev.3 (**03.04.09**); management is enforced through AC least-privilege/separation-of-duties, allow-lists, and continuous monitoring (03.01.05/06/07, 03.04.08, 03.12.03).

NIST.SP.800-171r3

5. **Two brand-new CM requirements**: **03.04.11 Information Location** (know exactly where CUI resides) and **03.04.12 High-Risk Areas** (pre-configured/travel-hardened builds with post-return actions).

NIST.SP.800-171r3

Conflicts (Interpretation or Alignment Friction)

- **3.4.7 (Rev.2) vs. 03.04.06/08 (Rev.3)**: Some implementations treated 3.4.7 as a distinct "harden ports/services" control. Rev.3 distributes those expectations between **Least Functionality** and **Authorized Software** while marking **03.04.07** withdrawn—this can look like a "gap" if you search only by IDs. Cross-reference confirms coverage.

NIST.SP.800-171r3

- **3.4.9 (Rev.2) dropped**: Teams may expect a 1:1 successor. Rev.3 resolves it by **policy/process** controls in AC/CA and allow-lists, not a CM-family ID.

NIST.SP.800-171r3

- **Terminology tightening**: Rev.3 consistently uses "system" and introduces ODPs (organization-defined parameters) for frequencies/scope, which may change assessment evidence expectations relative to Rev.2 text.

NIST.SP.800-171r3

Verification note: Control coverage was reconciled against **Table 7 – Configuration Management (CM)** in Rev.3 (complete list of 03.04.01-.12 and tailoring) and the corresponding Rev.3 §3.4 control language; Rev.2 §3.4 and Appendix D/E tables were used to confirm Rev.2 scope and mappings. **Counts match**: Rev.2 CM has **9** requirements (3.4.1–3.4.9); Rev.3 enumerates **12** items (03.04.01–03.04.12) with **2 withdrawn** (03.04.07, 03.04.09) and **10 active**.

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r2

NIST.SP.800-171r2

Gaps (What organizations commonly miss when moving to Rev.3 CM)

- **Allow-listing by default** (03.04.08): Many programs still rely on blacklisting; Rev.3's allow-listing is stricter and needs tooling/process updates.

NIST.SP.800-171r3

- **Inventory as a living artifact** (03.04.10): Event-driven updates (installs/removals/updates) must be proven, not just scheduled.

NIST.SP.800-171r3

- **CUI location traceability** (03.04.11): Requires documented linkage of **where** CUI is processed/stored to specific components and users.

NIST.SP.800-171r3

- **Travel/high-risk configurations** (03.04.12): Often absent; Rev.3 expects defined hardened builds and post-travel actions.

NIST.SP.800-171r3

- **Post-change verification** (03.04.04.b): Change processes frequently stop at "approve & implement" without documenting that controls still satisfy requirements afterward.

NIST.SP.800-171r3

Recommendations (Actionable steps to align with Rev.3)

1. **Split artifacts**: Maintain **separate** documents for **Baseline Configuration (03.04.01)** and **Component Inventory (03.04.10)** with ODP-defined review frequencies and install/remove/update triggers.

NIST.SP.800-171r3

NIST.SP.800-171r3

2. **Move to allow-lists**: Replace blacklisting policies with platform-appropriate **application allow-listing**; define ODP review cadence and approval workflow for changes to the allow-list.

NIST.SP.800-171r3

3. **Harden Least Functionality**: Embed periodic reviews (ODP), and automated checks for ports/protocols/services alignment with authorized lists; document disable/remove actions.

NIST.SP.800-171r3

4. **Document CUI location**: Stand up a **CUI location register** linking datasets ↔ systems/components ↔ users/roles; integrate with inventory and data-flow diagrams.

NIST.SP.800-171r3

5. **Travel profiles**: Define **high-risk travel** system builds (e.g., minimal apps, stricter configs) and post-return actions (e.g., reimage, forensics, attestations).

NIST.SP.800-171r3

6. **Change-control closure**: Add an explicit **post-implementation verification** step to change records to show controls remain satisfied (03.04.04.b).

NIST.SP.800-171r3

7. **Retire 3.4.9 evidence**: Migrate “user-installed software” checks into: least privilege/separation-of-duties (**03.01.05/06/07**), allow-listed software (**03.04.08**), and monitoring (**03.12.03**). Update policies, SSP, and POA&M accordingly.

NIST.SP.800-171r3

NIST.SP.800-171r3

Brief - Identification & Authentication (IA)

Below is the **Identification & Authentication (IA)** crosswalk ("delta document") between **NIST SP 800-171 Rev. 2 §3.5** and **NIST SP 800-171 Rev. 3 §03.05**. In short, Rev. 3 separates user and device identity, **broadens MFA and replay-resistance to all access (not just network)**, modernizes password policy to a **ban-list + cryptographic handling** model, **adds re-authentication** and **introduces an explicit Authenticator Management requirement**, while Rev. 2's "disable identifiers after inactivity" is **moved to Access Control (AC)** in Rev. 3. Coverage and mappings are validated against Rev. 2 Chapter Three and Appendices D/E, and Rev. 3 Section 3 and Appendix C (Table 9).

NIST.SP.800-171r2

NIST.SP.800-171r2

NIST.SP.800-171r3

Evidence Table — IA Crosswalk (Rev. 2 ↔ Rev. 3)

Legend: Each row aligns a Rev. 2 requirement with its closest Rev. 3 counterpart(s). "—" means no direct counterpart in that revision's IA family (may be moved or withdrawn).

Rev 2 (3.5.x)	Rev 3 (03.05.xx)	Explain the Difference
3.5.1 Identify system users, processes, and devices. NIST.SP.800-171r2	**03.05.01** User Identification & Authentication; **03.05.02** Device Identification & Authentication. NIST.SP.800-171r3	Rev. 3 **splits user vs. device** and adds **re-authentication triggers** in 03.05.01(b). NIST.SP.800-171r3
3.5.2 Authenticate identities of users/processes/devices before access. NIST.SP.800-171r2	**03.05.01** (users) + **03.05.02** (devices). NIST.SP.800-171r3	Same intent, now **explicitly separated**; user side adds **re-auth**. NIST.SP.800-171r3
3.5.3 MFA for local & network **privileged**, and **network** non-privileged accounts. NIST.SP.800-171r2	**03.05.03** MFA for **privileged and non-privileged accounts** (no "network" qualifier). NIST.SP.800-171r3	Rev. 3 **broadens MFA** to **all access** (local + network) for both

Rev 2 (3.5.x)	Rev 3 (03.05.xx)	Explain the Difference
		account types; simpler statement.
3.5.4 Replay-resistant mechanisms for **network** access to privileged & non-privileged accounts. NIST.SP.800-171r2	**03.05.04** Replay-resistant mechanisms for access to privileged & non-privileged accounts. NIST.SP.800-171r3	Rev. 3 removes the "network" qualifier—**applies to all access**.
3.5.5 Prevent reuse of identifiers for a defined period. NIST.SP.800-171r2	**03.05.05** Identifier Management (incl. authorization to assign IDs, selection, **prevent reuse**, and **identify user status**). NIST.SP.800-171r3	Rev. 3 keeps "no reuse" and **adds** governance (who can assign), selection rules, and a new element to **tag user status** (e.g., contractor).
3.5.6 Disable identifiers after a period of inactivity. NIST.SP.800-171r2	**Moved to AC**: **03.01.01.f.2** (disable inactive accounts), plus **03.01.10** device lock & related inactivity behaviors. NIST.SP.800-171r3 NIST.SP.800-171r3	Requirement **moved out of IA**; now handled under **Account Management** and device/session controls.
3.5.7 Enforce minimum password complexity & character change on creation. NIST.SP.800-171r2	**03.05.07** Password Management (ban-list checks; crypto transport/storage; first-use after recovery; **ODP-defined composition/complexity**). NIST.SP.800-171r3	Rev. 3 **modernizes** password policy (emphasizes **ban-lists** and cryptographic handling); composition rules become **organization-defined parameters (ODPs)**.
3.5.8 Prohibit password reuse for N generations.	**03.05.07** (no explicit "generational history" requirement).	Rev. 3 **drops explicit history-count**; orgs can

Rev 2 (3.5.x)	Rev 3 (03.05.xx)	Explain the Difference
NIST.SP.800-171r2	NIST.SP.800-171r3	still set such rules via ODPs if desired.
3.5.9 Allow temporary passwords with immediate change to permanent. NIST.SP.800-171r2	**03.05.07.e** change on first use **after account recovery**; **03.05.12.d** change default authenticators at first use. NIST.SP.800-171r3 NIST.SP.800-171r3	Rev. 3 **splits** this concept between **recovery** and **default credentials**; intent preserved with updated phrasing.
3.5.10 Store & transmit only **cryptographically-protected** passwords. NIST.SP.800-171r2	**03.05.07.c–d** (crypto for transmission & storage). NIST.SP.800-171r3	Rev. 3 consolidates into Password Management.
3.5.11 Obscure feedback of authentication info. NIST.SP.800-171r2	**03.05.11** Authentication Feedback. NIST.SP.800-171r3	Substantively unchanged.
—	**03.05.01(b) Re-authentication** under defined circumstances. NIST.SP.800-171r3	**New in Rev. 3 IA**: explicit re-auth triggers (e.g., role change, privileged actions).
—	**03.05.06 Withdrawn** (consistency with SP 800-53). NIST.SP.800-171r3	Placeholder only; **no requirement**.
—	**03.05.08 Withdrawn**. NIST.SP.800-171r3	Placeholder only; **no requirement**.
—	**03.05.09 Withdrawn**. NIST.SP.800-171r3	Placeholder only; **no requirement**.

Rev 2 (3.5.x)	Rev 3 (03.05.xx)	Explain the Difference
—	**03.05.10 Withdrawn — incorporated into 03.05.07**. NIST.SP.800-171r3	Clarifies consolidation into Password Management.
—	**03.05.12 Authenticator Management** (verify identity before issuance; initial content; procedures; **change defaults at first use**; periodic refresh; protect content). NIST.SP.800-171r3	**New, explicit** lifecycle controls for authenticators (beyond passwords), aligning to SP 800-53 IA-05. Rev. 2 only implied pieces in discussions.

Coverage checks:

• Rev. 2 IA contains **3.5.1–3.5.11** (11 requirements). All are mapped above from Chapter Three.

NIST.SP.800-171r2

NIST.SP.800-171r2

• Rev. 3 IA lists **03.05.01–03.05.12** (with 06/08/09/10 withdrawn), confirmed in **Appendix C, Table 9**.

NIST.SP.800-171r3

• Rev. 3 movement of inactivity disablement to **AC 03.01.01** verified in AC family text and Table 3.

NIST.SP.800-171r3

NIST.SP.800-171r3

Delta Statement (IA)

Rev. 3 **clarifies and tightens** identity and authentication by (1) **splitting** user vs. device identification (**03.05.01/02**) and adding **re-authentication** triggers; (2) **broadening** MFA (**03.05.03**) and **replay-resistance** (**03.05.04**) to **all** access, not only network; (3)

modernizing password policy (**03.05.07**) with **ban-list checks** and explicit crypto handling, making composition/complexity **organization-defined**; (4) adding a new, explicit **Authenticator Management** lifecycle (**03.05.12**); and (5) **relocating** inactivity/disablement from IA (**3.5.6**) to **Access Control Account Management** (**03.01.01**), keeping it in scope but outside the IA family.

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

Conflicts

- **Password policy model:** Rev. 2 mandates **character changes** and **history counts** (3.5.7–3.5.8), while Rev. 3 prioritizes **ban-lists** and crypto handling; composition and history are **optional via ODPs**.

NIST.SP.800-171r2

NIST.SP.800-171r3

- **Scope qualifiers:** Rev. 2 ties MFA and replay-resistance to **network** access (3.5.3–3.5.4). Rev. 3 removes that qualifier, implying **all access paths**.

NIST.SP.800-171r2

NIST.SP.800-171r2

NIST.SP.800-171r3

- **Location of inactivity control:** Rev. 2 houses inactivity/disablement under **IA** (3.5.6); Rev. 3 moves it to **AC** (03.01.01).

NIST.SP.800-171r2

NIST.SP.800-171r3

Gaps (to address when migrating from Rev. 2 → Rev. 3)

- **Authenticator lifecycle not explicit in Rev. 2:** Rev. 3 **03.05.12** adds concrete distribution, default change, refresh, and protection steps. Plan to implement these if not already present.

NIST.SP.800-171r3

- **Re-authentication events:** New in **03.05.01(b)**; define organizational triggers.

NIST.SP.800-171r3

- **Identifier management governance: 03.05.05** adds authorization-to-assign and user-status tagging; ensure procedures and attributes exist.

NIST.SP.800-171r3

- **Account inactivity:** If you previously met **3.5.6** only within IA, ensure compliance now resides under **AC 03.01.01/03.01.10**.

NIST.SP.800-171r3

NIST.SP.800-171r3

Recommendations

1. **Policy updates**
    - Update your **IA policy** to reflect **03.05.01–12** structure; add **re-authentication** conditions and **Authenticator Management** procedures.

NIST.SP.800-171r3

NIST.SP.800-171r3

    - Move “inactivity disablement” language from IA to **Account Management (AC)** procedures.

NIST.SP.800-171r3

2. **MFA scope**
    - Enforce MFA for **all** privileged and non-privileged account access (local & network). This aligns controls and simplifies exceptions.

NIST.SP.800-171r3

3. **Password management modernization**

- Implement a **banned-password list**; ensure **crypto in transit & at rest** for passwords; set **ODP** values for composition/complexity and any history you still require.

NIST.SP.800-171r3

4. **Identifier governance**
    - Formalize who may **assign identifiers**, **prevent reuse** periods, and add **user-status** attributes (e.g., contractor).

NIST.SP.800-171r3

5. **Validation against mappings**
    - Keep **Appendix C Table 9** (Rev. 3) and **Appendix D/E** (Rev. 2) handy as your authoritative mapping checkpoints during audits.

NIST.SP.800-171r3

NIST.SP.800-171r2

Brief - Incident Response (IR)

You asked for a Rev 2 ↔ Rev 3 crosswalk for the **Incident Response (IR)** family, using the same three-column layout as before. Verified coverage shows **Rev 2 contains 3 IR requirements (3.6.1–3.6.3)** and **Rev 3 contains 5 IR requirements (03.06.01–03.06.05)**. Rev 3 makes **training** and an **incident response plan** explicit requirements and folds **assistance** into a consolidated monitoring/reporting requirement.

NIST.SP.800-171r2

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

Evidence Table — IR Family Crosswalk (Rev 2 ↔ Rev 3)

Rev 2 Control (exact text)	**Rev 3 Control (exact text)**	**Explain the Difference**
3.6.1 — *Establish an operational incident-handling capability … including preparation, detection, analysis, containment, recovery, and user response activities.* NIST.SP.800-171r2	**03.06.01 Incident Handling** — *Implement an incident-handling capability … consistent with the incident response plan and including preparation, detection and analysis, containment, eradication, and recovery.* NIST.SP.800-171r3	Substantively aligned. Rev 3 ties handling to the **IR plan** and explicitly adds **eradication**; **"user response activities"** are removed here and addressed elsewhere.
3.6.2 — *Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.*	**03.06.02 Incident Monitoring, Reporting, and Response Assistance** — *(a) Track and document incidents; (b) report suspected incidents within [org-defined time period]; (c) report to [org-defined*	Rev 3 **expands** Rev 2 by formally adding **monitoring** sources, **org-defined timelines/authorities**, and an **explicit support resource** for user assistance (help desk/forensics). Rev 2

Rev 2 Control (exact text)	Rev 3 Control (exact text)	Explain the Difference
NIST.SP.800-171r2	*authorities]; (d) provide an incident response support resource (advice/assistance).* NIST.SP.800-171r3	mentioned assistance only in discussion, not as a standalone requirement.
3.6.3 — *Test the organizational incident response capability.* NIST.SP.800-171r2	**03.06.03 Incident Response Testing** — *Test the effectiveness of the incident response capability [org-defined frequency].* NIST.SP.800-171r3	Equivalent intent; Rev 3 adds **organization-defined frequency** and clarifies acceptable test methods (e.g., tabletop, simulations).
(no separate Rev 2 control; training noted only within 3.6.1 discussion) NIST.SP.800-171r2	**03.06.04 Incident Response Training** — role-based training with defined onboarding window, change-driven updates, and [org-defined] refresh frequency. NIST.SP.800-171r3	**New explicit requirement in Rev 3.** Rev 2 referenced IR training in narrative; Rev 3 makes it **mandatory** with timing parameters.
(no separate Rev 2 control; planning mapped as IR-8 "Plan" in Rev 2 tailoring table but not a 171 requirement) NIST.SP.800-171r2	**03.06.05 Incident Response Plan** — develop, distribute, update, and protect the IR plan; define reportable incidents and information sharing/roles. NIST.SP.800-171r3	**New explicit requirement in Rev 3.** Rev 2 listed **IR-8 Plan** only in the SP 800-53 tailoring matrix (NFO), not as a 800-171 requirement. Rev 3 elevates it into the core 171 requirements.

Verification note: Rev 3's Appendix C mapping confirms the five IR requirements (03.06.01–03.06.05) and their 800-53 lineage (IR-01..IR-08).

NIST.SP.800-171r3

Delta Statement — What's New/Different in Rev 3 (IR)

1. **Two new explicit requirements:**
   • **03.06.04 Incident Response Training** (role-based; onboarding and periodicity are organization-defined).

NIST.SP.800-171r3

• **03.06.05 Incident Response Plan** (documented, distributed, updated, protected).

NIST.SP.800-171r3

2. **Consolidated monitoring/reporting/assistance:**
   Rev 3's **03.06.02** merges monitoring and reporting with a **mandated support resource** and adds **organization-defined reporting timelines/authorities**. Rev 2 required tracking/reporting but did not mandate a support resource or timing parameters.

NIST.SP.800-171r3

NIST.SP.800-171r2

3. **Refined handling lifecycle:**
   Eradication is called out explicitly in **03.06.01**, and incident handling is required to be **consistent with the IR plan**. Rev 2 listed recovery and "user response activities"; Rev 3 moves user assistance under 03.06.02.

NIST.SP.800-171r3

NIST.SP.800-171r2

4. **Parameterized obligations:**
   Rev 3 introduces **[Assignment: organization-defined]** placeholders (e.g., training frequency, reporting windows, testing cadence), which you must define and implement.

NIST.SP.800-171r3

Conflicts

- **Where "assistance" lives:** Rev 2 mentions assistance in the **3.6.1 discussion**; Rev 3 moves it to a **formal requirement** under **03.06.02(d)**. Ensure your cross-references don't double-count the activity.

NIST.SP.800-171r2

NIST.SP.800-171r3

Gaps to Address When Moving from Rev 2 → Rev 3

- **No standalone IR training control in Rev 2** → must create and schedule **role-based IR training** per **03.06.04**.

NIST.SP.800-171r3

- **No standalone IR plan control in Rev 2** → must **author, distribute, maintain, and protect** an **IR plan** per **03.06.05**.

NIST.SP.800-171r3

- **Timelines/authorities undefined** → define **reporting timeframes** and **authorities** and stand up a **support resource** per **03.06.02**.

NIST.SP.800-171r3

- **Lifecycle terminology** → update procedures to include explicit **eradication** in the IR lifecycle per **03.06.01**.

NIST.SP.800-171r3

Recommendations

1. **Publish an IR Plan** aligned to 03.06.05 (define reportable incidents, roles, sharing rules; protect and maintain it).

NIST.SP.800-171r3

2. **Stand up a user support resource** (ticketing/help desk/forensics on-call) and codify **reporting windows & authorities** for 03.06.02.

NIST.SP.800-171r3

3. **Build a role-based IR training program** with onboarding and periodic refresh cycles per 03.06.04.

NIST.SP.800-171r3

4. **Update playbooks** to include **eradication** and reference the IR plan, satisfying 03.06.01.

NIST.SP.800-171r3

5. **Set a testing cadence** (e.g., annual tabletop plus simulation) to meet 03.06.03 and gather lessons learned.

NIST.SP.800-171r3

Brief — Maintenance (MA) Crosswalk (Rev 2 → Rev 3)
All six Rev 2 Maintenance requirements (3.7.1–3.7.6) are accounted for in Rev 3. Three Rev 3 items are marked *Withdrawn* with pointers to where the content moved (or recategorized as NCO), and three Rev 3 items (03.07.04–.06) remain active—with notable expansions: explicit media-inspection language is retained; nonlocal maintenance now explicitly covers *external or internal networks* and adds *replay resistance*; maintenance-personnel oversight is expanded to require authorization processes and maintained lists; and Rev 2's off-site sanitization moved to Media Protection (03.08.03). Verification: mappings below were checked against Rev 2 Ch. 3 and App. D and Rev 3 Sec. 3 and App. C tables for MA/MP families.

Evidence Table — Maintenance (MA)

Rev 2 (Control & text)	Rev 3 (Control & text)	Explain the Difference
3.7.1 — *Perform maintenance on organizational systems.* NIST.SP.800-171r2	**03.07.01** — *Withdrawn (recategorized as NCO).* NIST.SP.800-171r3	General maintenance is no longer a confidentiality-focused 171 requirement; it's out-of-scope per Rev 3 tailoring (NCO).
3.7.2 — *Provide controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance.* NIST.SP.800-171r2	**03.07.02** — *Withdrawn; incorporated into* **03.07.04** (*Maintenance Tools*) **and 03.07.06** (*Maintenance Personnel*). NIST.SP.800-171r3	Rev 3 splits Rev 2's combined tool/personnel requirement: tools are covered in 03.07.04 and authorization/supervision in 03.07.6.
3.7.3 — *Ensure equipment removed for off-site maintenance is sanitized of any CUI.* NIST.SP.800-171r2	**03.07.03** — *Withdrawn; incorporated into* **03.08.03 Media Sanitization** (MP family).	The sanitization requirement moved from MA to MP. The operative Rev 3 requirement is 03.08.03.
3.7.4 — *Check media containing diagnostic*	**03.07.04(b)** — *Check media with diagnostic and test*	Substantively retained under 03.07.04 (Maintenance Tools);

Rev 2 (Control & text)	Rev 3 (Control & text)	Explain the Difference
and test programs for malicious code before use. NIST.SP.800-171r2	*programs for malicious code before it is used in the system.* NIST.SP.800-171r3	Rev 3 adds discussion and examples of media inspection (e.g., hashes/signatures). NIST.SP.800-171r3
3.7.5 — *Require multifactor authentication to establish nonlocal maintenance sessions via external network connections and terminate when complete.* NIST.SP.800-171r2	**03.07.05(a–c)** — *Approve & monitor nonlocal maintenance; implement MFA* ***and replay resistance****; terminate sessions/network connections when complete.* Also clarifies **external or internal networks**. NIST.SP.800-171r3	Rev 3 broadens scope from "external" to **external or internal** networks and explicitly adds **replay resistance**; also requires approval/monitoring.
3.7.6 — *Supervise maintenance activities of personnel without required access authorization.* NIST.SP.800-171r2	**03.07.06(a–d)** — *Authorize maintenance personnel; maintain a list; verify non-escorted personnel have required authorizations; designate qualified supervisors with required access.* NIST.SP.800-171r3	Rev 3 expands supervision into a fuller authorization and oversight process (lists, verification, designated supervisors).
— *(no explicit Rev 2 equivalent; partial relation to 3.7.3)*	**03.07.04(c)** — *Prevent removal of maintenance equipment containing CUI (verify no CUI, sanitize/destroy, or retain).* NIST.SP.800-171r3	New explicit egress-prevention step in the tools requirement; Rev 2 focused on sanitization **once removed**; Rev 3 adds **prevent removal** unless conditions are met.

Rev 2 (Control & text)	Rev 3 (Control & text)	Explain the Difference
— *(no explicit Rev 2 equivalent)*	**03.07.05(a)** — *Approve and monitor nonlocal maintenance and diagnostic activities.* NIST.SP.800-171r3	Approval/monitoring is now explicit for nonlocal maintenance; Rev 2 did not directly require approval/monitoring in 3.7.5.
— *(no explicit Rev 2 equivalent beyond supervision)*	**03.07.06(a–b)** — *Establish authorization process and maintain list of authorized maintenance orgs/personnel.* NIST.SP.800-171r3	New explicit process and inventory/listing requirements for maintenance personnel.
(Context for policy mapping)	**MA-01 → 03.15.01 (Policy & Procedures)** (family-wide policy anchor) and **MA-02/MA-06** marked **NCO** in Rev 3 tables. NIST.SP.800-171r3	Rev 3 centralizes "policy & procedures" at 03.15.01; general "controlled/timely maintenance" controls are NCO (not in scope for confidentiality-only).

Conflicts (what could be misread or contradicted)

- **Family relocation:** Teams may still look for off-site sanitization in MA; it now lives in **MP 03.08.03**. Using the old family could create documentation discrepancies.
- **Network scope wording:** Rev 2 scoped nonlocal maintenance to "external network connections"; Rev 3 covers **external or internal** networks (broader), and adds **replay resistance** to MFA—this can contradict older SOPs that assumed internal networks were out-of-scope.

Gaps (coverage and verification notes)

- **Coverage check:** All **Rev 2 3.7.1–3.7.6** are mapped above, and all **Rev 3 03.07.01–03.07.06** are represented (including withdrawn notes and where content moved). Verified against Rev 3 Table 11 (MA) and the Rev 3 MA/MP text.

- **ODPs:** No organization-defined parameters are specified for 03.07.* in Rev 3 Appendix D. (ODPs appear for other families; none listed for MA.)

NIST.SP.800-171r3

- **Policy anchor:** If you previously tied an MA-specific policy to 3.7.1, move that into your unified **03.15.01 Policy and Procedures** control in Rev 3.

NIST.SP.800-171r3

Recommendations (actionable deltas)

1. **Update SSP cross-references:** Move *off-site maintenance sanitization* content from MA to **MP 03.08.03**; note linkage from 03.07.03 (withdrawn) in your delta log.
2. **Harden nonlocal maintenance:** Require **MFA + replay resistance** for any nonlocal maintenance (internal *or* external network), and document **approval/monitoring** of these sessions. Update procedures and tooling accordingly.

NIST.SP.800-171r3

3. **Tighten tool controls:** Implement an allow-list and periodic reviews for maintenance tools; **inspect media** (hash/signature checks) before use.
4. **Control equipment egress:** Enforce **03.07.04(c)**—verify no CUI, sanitize/destroy, or retain maintenance equipment; add this step to exit/escort checklists.

NIST.SP.800-171r3

5. **Formalize maintenance personnel governance:** Stand up an authorization process and maintain an **authorized-personnel list**; require verification of non-escorted personnel and designate supervisors with required access and competence.

NIST.SP.800-171r3

6. **Housekeeping:** Retire Rev 2 MA statements that are now **NCO** in Rev 3 (e.g., general "perform maintenance"), and reference the unified **03.15.01** policy requirement where applicable.

NIST.SP.800-171r3

Delta Statement — What's New/Different in Rev 3 (Maintenance)

- **Three MA items withdrawn:** 03.07.01 (*recategorized as NCO*), 03.07.02 (*split into 03.07.04 & 03.07.06*), 03.07.03 (*moved to MP 03.08.03*).

NIST.SP.800-171r3

- **Nonlocal maintenance strengthened:** Now explicitly covers **internal** networks and requires **MFA + replay resistance**, plus approval/monitoring. Rev 2 required MFA for *external* only and didn't call out replay resistance.
- **Personnel governance expanded:** Adds authorization process and maintained list; requires verifying non-escorted personnel and designating qualified supervisors. Rev 2 only required supervision of unauthorized personnel.

NIST.SP.800-171r3

- **Equipment removal control added:** New explicit prohibition/conditions for removing maintenance equipment containing CUI (verify/sanitize/destroy/retain). Rev 2 focused on sanitization **once off-site**.

NIST.SP.800-171r3

- **Policy centralization:** MA policy/procedure content maps to the family-agnostic **03.15.01** control; general "controlled/timely maintenance" items are NCO in Rev 3.

NIST.SP.800-171r3

Brief — Media Protection (MP) Crosswalk (NIST SP 800-171 Rev. 2 → Rev. 3)
Rev. 3 retains the Media Protection family but renumbers controls from **3.8.x** to **03.08.xx**, clarifies scope, introduces organization-defined parameters (ODPs) where applicable, consolidates two removable-media requirements into one, and moves the "crypto during transport" requirement out of MP into System & Communications Protection (SC). A new Rev. 3 requirement explicitly mandates cryptographic protection for **backup** CUI.

NIST.SP.800-171r3

NIST.SP.800-171r3

Evidence Table — Media Protection (MP)

Rev 2 (3.8.x)	Rev 3 (03.08.xx)	Explain the Difference
3.8.1 Protect (physically control and securely store) system media containing CUI (paper & digital). NIST.SP.800-171r2	**03.08.01 Media Storage** – "Physically control and securely store system media that contain CUI"; expands examples of storage media and describes secure storage/controlled areas. NIST.SP.800-171r3	**Substantively equivalent.** Rev. 3 adds examples and explanatory text (secure storage, controlled areas) but no new obligation.
3.8.2 Limit access to CUI on system media to authorized users. NIST.SP.800-171r3	**03.08.02 Media Access** – Restrict access to CUI on system media to authorized personnel/roles; notes encryption for digital media ties to 03.13.08. NIST.SP.800-171r3	**Equivalent with clarification.** Rev. 3 explicitly points to crypto-at-rest/transit requirement in SC (03.13.08) for digital media.
3.8.3 Sanitize or destroy system media containing CUI before disposal or reuse. NIST.SP.800-171r2	**03.08.3 Media Sanitization** – Same objective; clarifies it applies to removable/non-removable media and lists techniques (crypto erase, clear, purge, destroy). NIST.SP.800-171r3	**Equivalent with elaboration.** Scope and techniques are spelled out; intent unchanged.

Rev 2 (3.8.x)	Rev 3 (03.08.xx)	Explain the Difference
3.8.4 Mark media with necessary CUI markings and distribution limitations. NIST.SP.800-171r2	**03.08.04 Media Marking** – Same function; reiterates that marking is human-readable and references CUI program. NIST.SP.800-171r3	**Equivalent.** Editorial clarifications only.
3.8.5 Control access and maintain accountability for media during transport outside controlled areas. NIST.SP.800-171r2	**03.08.05 Media Transport** – Adds **(c)** "document activities associated with the transport," retains protection/accountability, and notes cryptography/locked containers. NIST.SP.800-171r3	**Tightened.** Rev. 3 adds a **documentation** obligation for transport activities; otherwise consistent.
3.8.6 Implement cryptographic mechanisms to protect confidentiality of CUI stored on digital media during transport unless protected by physical safeguards. NIST.SP.800-171r2	**03.08.06 Withdrawn** – expressly **addressed by 03.13.08 (Transmission and Storage Confidentiality)** in SC family. NIST.SP.800-171r3 NIST.SP.800-171r3	**Relocated/Consolidated.** The crypto requirement is no longer in MP; it is covered centrally by **03.13.08** (for both transmission and storage).
3.8.7 Control the use of removable media on system components. NIST.SP.800-171r2	**03.08.07 Media Use (a)** – "Restrict or prohibit the use of **[ODP: org-defined types]** of system media." NIST.SP.800-171r3	**Equivalent with ODP.** Rev. 3 introduces an **ODP** to tailor which media types are restricted/prohibited.

Rev 2 (3.8.x)	Rev 3 (03.08.xx)	Explain the Difference
3.8.8 Prohibit use of portable storage devices with no identifiable owner. NIST.SP.800-171r2	**03.08.07 Media Use (b)** – "Prohibit use of removable system media without an identifiable owner." **03.08.08 Withdrawn – incorporated into 03.08.07.** NIST.SP.800-171r3	**Merged.** Rev. 2's 3.8.7 and 3.8.8 are combined in **03.08.07**; **03.08.08** exists only as a note marking the consolidation.
3.8.9 Protect the confidentiality of backup CUI at storage locations. NIST.SP.800-171r2	**03.08.09 System Backup – Cryptographic Protection** – (a) Protect confidentiality of backup info **and** (b) **implement cryptographic mechanisms** to prevent unauthorized disclosure at backup storage locations (ties to 03.13.11). NIST.SP.800-171r3	**Strengthened.** Rev. 3 makes **encryption explicit** for backup CUI and references cryptographic control 03.13.11.

Verification note (coverage): This crosswalk covers all nine MP requirements in Rev. 2 (**3.8.1–3.8.9**) and all Rev. 3 MP requirements (**03.08.01–03.08.09**, including the two **Withdrawn** items) with their current placement/wording in Rev. 3 and any relocations to SC (03.13.08).

NIST.SP.800-171r2

NIST.SP.800-171r2

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

Delta Statement — What's New/Different in Rev. 3 (MP)

1. **Numbering & structure:** MP controls renumber from **3.8.x** to **03.08.xx** with expanded discussions; ODPs appear where tailoring makes sense (e.g., media types in **03.08.07(a)**).

NIST.SP.800-171r3

2. **Media transport: New documentation duty**—organizations must **document transport activities** for CUI media under **03.08.05(c)**.

NIST.SP.800-171r3

3. **Crypto during transport/storage:** The Rev. 2 media-family requirement **3.8.6** is **withdrawn** in MP and **moved to SC** as **03.13.08 Transmission and Storage Confidentiality**, which centralizes crypto requirements for **both transmission and storage**.

NIST.SP.800-171r3

NIST.SP.800-171r3

4. **Removable media consolidation:** Rev. 2 **3.8.7** (control removable media) and **3.8.8** (prohibit media without identifiable owner) are **merged** into **03.08.07**, and **03.08.08** is marked **Withdrawn** to reflect the consolidation.

NIST.SP.800-171r3

5. **Backups hardened:** Rev. 2 **3.8.9** becomes **03.08.09 System Backup – Cryptographic Protection**, explicitly **requiring encryption** for backup CUI and referencing cryptographic controls (03.13.11).

NIST.SP.800-171r3

Conflicts (Noted or Potential)

- **Family boundary vs. crypto placement:** Teams used to satisfying encryption for media transport under **3.8.6** may miss it in Rev. 3 because it now lives under **SC (03.13.08)**, not MP. Ensure control owners are updated.

NIST.SP.800-171r3

- **Terminology alignment:** Rev. 3 consistently speaks to “system media” and ties cryptographic references to SC; ensure procedures and SSP language reflect the **renamed/renumbered** requirements.

NIST.SP.800-171r3

Gaps (to be addressed by the organization)

- **ODP values: 03.08.07(a)** requires an **organization-defined list of media types** to restrict/prohibit; if not set by your sponsor, you must set it locally and document in the SSP/ODP register.

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Media transport records:** If procedures/logs for **documenting transport activities** (03.08.05(c)) don't exist, they must be created (including fields like media ID, courier, dates/times, chain-of-custody).

NIST.SP.800-171r3

- **Backup encryption detail:** Confirm crypto mechanisms for **backup CUI** (03.08.09) and key management align with **03.13.11** (FIPS-validated cryptography recommended).

NIST.SP.800-171r3

NIST.SP.800-171r3

Recommendations

1. **Update the SSP cross-references:** Map Rev. 2 **3.8.6** controls and procedures to **03.13.08** and **03.13.11**; adjust ownership from MP to SC.

NIST.SP.800-171r3

NIST.SP.800-171r3

2. **Publish an ODP decision memo** for **03.08.07(a)** listing prohibited/restricted media (e.g., personal USBs, writable optical media) and permitted exceptions.

NIST.SP.800-171r3

3. **Add a media-transport log template** to satisfy **03.08.05(c)** (chain-of-custody, approvals, anomalies).

NIST.SP.800-171r3

4. **Harden backup protection** to **03.08.09** by enforcing encryption at backup targets (e.g., tape libraries, off-site vaults) and documenting HSM/key-management integrations.

NIST.SP.800-171r3

5. **Train control owners** on renumbering and merged controls (03.08.07), so assessments don’t misattribute evidence to outdated 3.8.7/3.8.8 references.

NIST.SP.800-171r3

Brief — Personnel Security (PS) crosswalk (Rev 2 → Rev 3)
All PS requirements in Rev 2 (two basics: 3.9.1 and 3.9.2; no derived) were located and mapped to Rev 3. Rev 3 keeps two PS requirements (03.09.01 and 03.09.02) and introduces an explicit cross-cutting "Policy and Procedures" requirement (03.15.01) that is sourced from PS-01 in the SP 800-53 moderate baseline and applies across families. Verification points are cited inline below.

Evidence Table — Rev 2 vs Rev 3 (Personnel Security)

Rev 2 Control	Rev 3 Control	Explain the Difference
3.9.1 – Screen individuals prior to authorizing access to organizational systems containing CUI. NIST.SP.800-171r2	**03.09.01 – Personnel Screening.** Requires screening prior to authorizing access *and* adds **rescreening** "in accordance with [organization-defined conditions]," making rescreening mandatory via an ODP. Also clarifies screening applies when *elevating* access. NIST.SP.800-171r3 The new ODP is explicitly listed for 03.09.01.b. NIST.SP.800-171r3	**Substance retained; scope tightened.** Rev 3 adds required **rescreening** (ODP) and clarifies timing/trigger ("prior to authorizing access" and on access elevation).
3.9.2 – Ensure systems containing CUI are protected during and after personnel actions (terminations and transfers). NIST.SP.800-171r2	**03.09.02 – Personnel Termination and Transfer.** Specifies **enumerated actions** at termination (disable access within an **ODP-defined time period**, revoke credentials, retrieve security-related property) and **defined checks** on transfer (confirm need; modify authorizations). NIST.SP.800-171r3 The ODP adds a concrete time parameter for disabling access.	**More prescriptive.** Rev 3 transforms a general safeguard into a checklist with an **ODP time window** and explicit actions for both termination and transfer.

Rev 2 Control	Rev 3 Control	Explain the Difference
	NIST.SP.800-171r3	
(No Rev 2 counterpart in PS family)	**03.15.01 – Policy and Procedures.** System-wide requirement to develop, disseminate, and periodically update policies and procedures that cover **each family** (including PS). NIST.SP.800-171r3 In Appendix C, **PS-01** in the SP 800-53 baseline is tailored **CUI → 03.15.01**, establishing the linkage for PS. NIST.SP.800-171r3	**New cross-cutting requirement.** Rev 3 makes written policy/procedure coverage explicit across families; Rev 2 treated much of this implicitly (e.g., via "NFO" in its tailoring tables), not as a numbered CUI requirement.

Notes used for verification: Rev 2 PS basics and "no derived" are in Ch. 3 (§3.9) and Appendix D Table D-9. Rev 3 PS text for 03.09.01–.02 appears in §3.9; ODPs for **03.09.01.b** and **03.09.02.a.01** are listed in Appendix D; the **PS-01 → 03.15.01** linkage is in Appendix C Table 16 and the 03.15.01 requirement text is in §3.15.

Delta Statement — What's new/different in Rev 3 (PS)

1. **Rescreening becomes explicit and parameterized.** Rev 3 adds **rescreening** of individuals based on **organization-defined conditions (ODP)**—a new requirement absent from Rev 2's 3.9.1.
2. **Termination/transfer actions are now prescriptive with a deadline.** Rev 3 requires disabling access **within an ODP-defined time period**, credential revocation, retrieval of security property, and documented adjustments on transfer—tightening Rev 2's broadly worded 3.9.2.
3. **Formal policy/procedure coverage is required across families.** Rev 3 introduces **03.15.01** (Planning family) that is explicitly sourced from **PS-01** and applies to PS as part of enterprise policy governance—this was not a numbered CUI requirement in Rev 2.

4. **Terminology alignment.** Rev 3 refers to "the **system**" (defined in Sec. 3 as the nonfederal system/components processing CUI) instead of Rev 2's "organizational systems containing CUI"—a wording change with equivalent scope per definition.

NIST.SP.800-171r3

Conflicts (none material)

- **Scope wording:** Rev 2's "organizational systems containing CUI" vs. Rev 3's "system" might appear narrower. The Rev 3 definition of "system" in Sec. 3 explicitly targets nonfederal systems/components that process, store, or transmit CUI; scope is effectively the same.

NIST.SP.800-171r3

Gaps to address when moving to Rev 3 (PS)

- **Set ODP values:**
  • **Rescreening conditions** for 03.09.01.b.

NIST.SP.800-171r3

• **Access-disable time window** for 03.09.02.a.01.

NIST.SP.800-171r3

- **Codify PS coverage in policy:** Ensure PS is explicitly covered under **03.15.01** policies and procedures, with review/update frequency specified.

NIST.SP.800-171r3

Recommendations

1. **Update HR + Security SOPs** to embed: (a) vetting prerequisites before account creation or privilege elevation; (b) **rescreening triggers** (e.g., role change to privileged, adverse events, inactivity) per 03.09.01.b; (c) a **hard SLA** (ODP) for disabling access at termination (e.g., immediate or ≤ 15 minutes).

2. **Revise access deprovisioning runbooks** to include credential revocation and retrieval of tokens/IDs/keys/manuals; require transfer checklists to reconfirm least-privilege and update badges/keys.

NIST.SP.800-171r3

3. **Publish and maintain PS policies** under **03.15.01** with an explicit review cadence (e.g., annually) and trace PS procedures to roles.

NIST.SP.800-171r3

Brief — Physical Security / Protection (PH/PE) Crosswalk (Rev 2 → Rev 3)
Below is a side-by-side alignment of **every** Physical Protection requirement in **NIST SP 800-171 Rev 2 §3.10** with the corresponding **Rev 3 §3.10** requirements. Rev 3 consolidates visitor control, physical access logging, and access device management into **03.10.07**, adds explicit **authorization list & credential issuance** (**03.10.01**), separates **cabling / transmission media protection** into **03.10.08**, and introduces organization-defined parameters (ODPs) for review cadence and triggers. (See Rev 2 Ch. 3 pp. 32–33; Rev 3 Sec. 3.10 pp. 50–53; Rev 3 Appendix tables mapping PE→03.10.*).

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

NIST.SP.800-171r3

Evidence Table — Physical Security / Protection Crosswalk

Rev 2 Control	Rev 3 Control(s)	Explain the Difference
3.10.1 Limit physical access to systems, equipment, and operating environments to authorized individuals. (Ch. 3 p. 32) NIST.SP.800-171r2	**03.10.01** Physical Access Authorizations; **03.10.07** Physical Access Control. (Sec. 3.10 pp. 50–53) NIST.SP.800-171r3 NIST.SP.800-171r3	Rev 3 **splits** the concept: **03.10.01** requires a maintained **authorized-access list**, issuing credentials, and **periodic reviews (ODP frequency)**; **03.10.07** covers **enforcement** at entry/exit points. Rev 2 implied both but did not require the list/credential issuance or ODP.
3.10.2 Protect and **monitor** the physical facility and **support infrastructure** (e.g., cabling). (Ch. 3 p. 32)	**03.10.02** Monitoring Physical Access; **03.10.08** Access Control for Transmission (cabling). (Sec. 3.10 pp. 51–53) NIST.SP.800-171r3	Rev 3 **separates** responsibilities: **03.10.02** adds **detect & respond to incidents** and requires **log reviews** at ODP-defined **frequencies/events**; **03.10.08** pulls out the cabling/transmission medium protection from Rev 2's broad 3.10.2.

Rev 2 Control	Rev 3 Control(s)	Explain the Difference
NIST.SP.800-171r2	NIST.SP.800-171r3	
3.10.3 Escort visitors and monitor visitor activity. (Ch. 3 p. 33) NIST.SP.800-171r3	**03.10.07(c)** Escort visitors & control visitor activity; (**03.10.03** is **withdrawn** and incorporated into 03.10.07). (Sec. 3.10 p. 53 and note) NIST.SP.800-171r3	Substantively the same, but **explicitly consolidated** into 03.10.07. Rev 3 clarifies that individuals with permanent physical access authorizations are **not** visitors.
3.10.4 Maintain **audit logs** of physical access. (Ch. 3 p. 33) NIST.SP.800-171r3	**03.10.07(b)** Maintain access logs; **03.10.02(b) review** logs per ODP frequency/events; (**03.10.04** withdrawn into 03.10.07). (Sec. 3.10 pp. 51–53) NIST.SP.800-171r3	Rev 3 keeps logging in **03.10.07**, and **adds** a required **review cadence & triggers** in **03.10.02** via ODPs—new specificity versus Rev 2's generic "maintain logs."
3.10.5 Control and manage **physical access devices** (keys, locks, combos, card readers). (Ch. 3 p. 33) NIST.SP.800-171r3	**03.10.07(d)** Secure keys, combinations, and other access devices; (**03.10.5** withdrawn into 03.10.07). (Sec. 3.10 p. 53) NIST.SP.800-171r3	Direct carryover, now **nested** in 03.10.07 with clearer scope.
3.10.6 Enforce safeguarding measures for CUI at **alternate work sites**. (Appendix D mapping + Ch. 3 p. 33) NIST.SP.800-171r2	**03.10.06** Alternate Work Site. (Sec. 3.10 p. 52) NIST.SP.800-171r3	Rev 3 keeps the requirement and **adds** specifics: define **which alternate sites are permitted** and apply **ODP-defined** security requirements; includes references to SP 800-46/114 for telework guidance.

Rev 2 Control	Rev 3 Control(s)	Explain the Difference
NIST.SP.800-171r3		
(No explicit Rev 2 row; implicit via 3.10.2's mapping to PE-5) NIST.SP.800-171r2	**03.10.07(e) Control physical access to output devices** (e.g., printers, scanners, displays) to prevent unauthorized CUI viewing. (Sec. 3.10 p. 53) NIST.SP.800-171r3	Rev 3 **makes explicit** output-device controls that Rev 2 handled only indirectly via the 3.10.2 mapping to **PE-5** in Appendix D; now spelled out with concrete examples (screen filters, device placement).
(Reference mapping confirmation)	**PE→03.10 mapping** (PE-02→03.10.01; PE-03/PE-05→03.10.07; PE-06→03.10.02; PE-04→03.10.08; PE-17→03.10.06). (Appendix Table 13) NIST.SP.800-171r3	Confirms Rev 3 **family coverage and numbering** for Physical/Environmental Protection controls and where Rev 2 concepts landed in Rev 3.

Delta Statement — What's New/Different in Rev 3 (Physical Security / Protection)

1. **Authorization list & credential issuance are now mandatory**: Rev 3 adds **03.10.01** requiring a maintained list of authorized individuals, issuance of authorization credentials, and **ODP-defined review frequency**—elements only implied in Rev 2's 3.10.1.

NIST.SP.800-171r3

2. **Monitoring now includes incident response and mandatory reviews**: **03.10.02** requires **detecting/responding** to physical security incidents and **reviewing access logs** at defined **frequencies and event-triggers (ODPs)**—stronger than Rev 2's "protect and monitor."

NIST.SP.800-171r3

3. **Cabling/transmission media split out**: Protection of distribution/transmission lines moved from the broad 3.10.2 into a dedicated **03.10.08**, with concrete examples (locked wiring closets, conduit, wiretap sensors).

NIST.SP.800-171r3

4. **Visitor control, access logs, and access devices consolidated**: Rev 2's **3.10.3–3.10.5** are **withdrawn** as stand-alone items and **incorporated** into **03.10.07** (visitor escort, access-log maintenance, securing keys/combos/devices). **03.10.07** also adds explicit **output-device** protections.

NIST.SP.800-171r3

5. **Alternate work sites clarified**: **03.10.06** retains Rev 2's expectation but adds **determination of allowed sites** and **ODP-defined security requirements**, with telework references.

NIST.SP.800-171r3

6. **Numbering & mappings updated**: Rev 3 aligns with **PE** controls in SP 800-53 as shown in **Appendix Table 13** (e.g., PE-02→03.10.01, PE-06→03.10.02).

NIST.SP.800-171r3

Conflicts (none material)

- **No substantive contradictions** between Rev 2 intent and Rev 3 outcomes were found. Rev 3 primarily **restructures** and **clarifies**—introducing ODPs and consolidations. Cross-checked against Rev 2 Ch. 3 text and Rev 3 Sec. 3.10 plus Appendix mappings.

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

Gaps / Edge Cases to Decide Locally

- **ODP values** to set for: access-list **review frequency** (03.10.01.c) and **log review frequency & event triggers** (03.10.02.b). Rev 3 requires you to **define** these.

NIST.SP.800-171r3

- **Output-device coverage**: Rev 2 programs that did not explicitly address printer/display **placement or screen filters** should add these per **03.10.07(e)**.

NIST.SP.800-171r3

- **Transmission-line protections**: Ensure controls on **wiring closets, spare jacks, conduit, tap sensors** are documented under **03.10.08**, not just facility controls.

NIST.SP.800-171r3

Recommendations

1. **Document the physical-access authorization list & credential process** and set an **ODP review cadence** (e.g., quarterly) for **03.10.01**.

NIST.SP.800-171r3

2. **Enhance monitoring SOPs** to include **incident detection/response steps** and **ODP-based log reviews** (e.g., daily automated review; immediate review on alarm). Map to **03.10.02**.

NIST.SP.800-171r3

3. **Update site standards** to explicitly control **output devices** (placement, filters, access controls) per **03.10.07(e)**.

NIST.SP.800-171r3

4. **Harden cabling/distribution** per **03.10.08**: lock closets, disable/lock spare jacks, use conduit/cable trays, deploy tap detection where feasible.

NIST.SP.800-171r3

5. **Define approved alternate work sites** and **ODP-defined safeguards** (e.g., locked room, visitor policy, clean-desk, shredder, no shoulder-surfing) for **03.10.06**.

NIST.SP.800-171r3

Brief — Risk Assessment (RA) family crosswalk (Rev 2 → Rev 3)
Rev 3 keeps the intent of Rev 2's RA controls but (1) makes risk assessments explicitly include **supply-chain risk** and periodic updates, (2) folds **remediation** into the vulnerability requirement and adds **monitoring** alongside scanning, and (3) introduces a new **Risk Response** requirement tied to POA&M decisions. I verified the control texts in Chapter 3 of both revisions and the RA mapping/tailoring tables.

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

Evidence Table — RA Controls (line up where possible)

Rev 2 control	Rev 3 control	Explain the difference
3.11.1 Risk Assessment — "Periodically assess the risk to organizational operations/assets/individuals resulting from system operation and CUI processing/storage/transmission." NIST.SP.800-171r2	**03.11.01 Risk Assessment** — "Assess the risk **(including supply chain risk)** of unauthorized disclosure of CUI; **update risk assessments** at an organization-defined frequency." NIST.SP.800-171r3	Substantively aligned, but Rev 3 (a) **explicitly adds supply-chain risk** and (b) requires **periodic updates** via an organization-defined parameter (ODP). Rev 3's discussion also stresses system boundary establishment. ODP for 03.11.01.b is listed in Appendix D. NIST.SP.800-171r3 NIST.SP.800-171r3
3.11.2 Vulnerability Scanning — "Scan for vulnerabilities periodically and when new vulnerabilities are identified." (Guidance references CVE/CWE/NVD/CVSS.)	**03.11.02 Vulnerability Monitoring and Scanning** — "**Monitor and scan** at an org-defined frequency and when new vulnerabilities	Rev 3 **adds "monitoring"** to scanning, **moves remediation into the same requirement**,

Rev 2 control	Rev 3 control	Explain the difference
NIST.SP.800-171r2	arise; **remediate** within org-defined response times; **update the vulnerabilities to be scanned** at an org-defined frequency." (Discussion again references CVE/CWE/NVD/CVSS.) NIST.SP.800-171r3	and introduces **ODPs** for scan frequency, response times, and update frequency. (ODPs for 03.11.02.a/.b/.c are enumerated in Appendix D.) NIST.SP.800-171r3
3.11.3 Remediate vulnerabilities in accordance with risk assessments. NIST.SP.800-171r2	**(Merged into 03.11.02; 03.11.03 is "Withdrawn").** NIST.SP.800-171r3	In Rev 3, the separate remediation control is **consolidated** into 03.11.02; 03.11.03 appears as **Withdrawn (incorporated into 03.11.02)**. NIST.SP.800-171r3
(No Rev 2 counterpart)	**03.11.04 Risk Response** — "Respond to findings from security assessments, monitoring, and audits," with POA&M considerations. NIST.SP.800-171r3	**New in Rev 3**: requires a defined **risk response** step prior to (or resulting in) POA&M entries; may avoid a POA&M if mitigated immediately. NIST.SP.800-171r3
(Rev 2 mapping note) 3.11.2 referenced **RA-5(5) Privileged Access** in 800-53 as related context; not a separate 171 requirement. NIST.SP.800-171r2	*(Rev 3 tailoring note)* 800-53 **RA-05(05) Privileged Access** is categorized **ORC (other related control)** — not required by 171r3. Table 18.	Clarifies that privileged-access scanning nuances are informative/related rather than direct CUI obligations in Rev 3.

Rev 2 control	Rev 3 control	Explain the difference
	NIST.SP.800-171r3	NIST.SP.800-171r3

Delta Statement — What's new/different in Rev 3 (RA)

1. **Supply-chain risk comes into scope of RA** — Rev 3 requires risk assessments to **include supply-chain risk** and to be **updated** at an organization-defined cadence.

NIST.SP.800-171r3

2. **Vulnerability "monitoring" + consolidated remediation** — Rev 3 changes "scan" to **"monitor and scan,"** and **merges remediation** into 03.11.02; the former standalone remediation control is **withdrawn** (03.11.03).

NIST.SP.800-171r3

NIST.SP.800-171r3

3. **New, explicit Risk Response step** — Rev 3 adds **03.11.04**, directing organizations to define and apply a **risk response** before deciding on POA&M entries (mitigate immediately where possible).

NIST.SP.800-171r3

4. **Organization-Defined Parameters (ODPs)** — Rev 3 introduces **ODPs** for RA, requiring you to set values for assessment **frequency**, scan **frequency**, **response times**, and update **frequency**. (See Appendix D entries for 03.11.01.b; 03.11.02.a/.b/.c.)

NIST.SP.800-171r3

Conflicts (none material)

- **Terminology/structure changes** (e.g., adding "monitoring," consolidating remediation, and new "Risk Response") modify layout but do **not** contradict Rev 2 intent to identify and address risk and vulnerabilities. Verified against Chapter 3 texts for both revisions and the RA tailoring table.

NIST.SP.800-171r2

NIST.SP.800-171r3

NIST.SP.800-171r3

Gaps to close before implementation / assessment

- **Set ODP values** for: risk-assessment update **frequency** (03.11.01.b), vulnerability **scan frequency**, **response times**, and **update frequency** (03.11.02.a/.b/.c). These are required to complete the Rev 3 requirements.

NIST.SP.800-171r3

- **Define a Risk Response process** that ties assessment/monitoring/audit findings to a decision path **before** POA&M creation (e.g., immediate mitigation vs. POA&M entry).

NIST.SP.800-171r3

- **Document supply-chain inputs** to RA (e.g., supplier reviews feeding RA per SR-06 reference in 03.11.01's sources).

NIST.SP.800-171r3

Recommendations

1. **Update your RA procedure** to explicitly include **supply-chain risk** factors and to **schedule updates** at your chosen cadence (documented as the ODP for 03.11.01.b).

NIST.SP.800-171r3

NIST.SP.800-171r3

2. **Unify vulnerability scanning + remediation** under one SOP that covers **monitoring**, **scan frequency**, **response times**, and **catalog updates**; record these as ODPs for 03.11.02.a/.b/.c.

NIST.SP.800-171r3

NIST.SP.800-171r3

3. **Establish a Risk Response playbook** describing when to **mitigate immediately** vs. **open a POA&M**, with accountable roles and escalation paths.

NIST.SP.800-171r3

4. **Align evidence artifacts** (risk register entries, scan results, remediation tickets, POA&Ms) to the new Rev 3 control IDs (03.11.01–.04) to streamline assessments.

NIST.SP.800-171r3

NIST.SP.800-171r3

Brief — Security Assessment & Monitoring (CA) Crosswalk (Rev 2 → Rev 3)
I aligned every Rev 2 "Security Assessment" control (3.12.1–3.12.4) to the Rev 3 "Security Assessment and Monitoring" family (03.12.01–03.12.05) and, where applicable, to Planning 03.15.02 (because Rev 3 relocates the SSP requirement). I verified coverage against the authoritative text in both PDFs and noted substantive deltas (scope, relocation, added ODPs, and the new Information Exchange requirement).

Evidence Table — Control-by-Control Comparison

Rev 2 control (verbatim gist)	**Rev 3 control (verbatim gist)**	**Explain the difference**
3.12.1 – "Periodically assess the security controls in organizational systems to determine if the controls are effective in their application." NIST.SP.800-171r2	**03.12.01 Security Assessment** – "Assess the **security requirements** for the system **and its environment of operation** [**ODP: frequency**] to determine if the requirements have been satisfied." NIST.SP.800-171r3	Scope shifts from assessing **controls** to assessing **requirements**, and explicitly includes the **environment of operation**; Rev 3 introduces an **organization-defined frequency** (ODP). NIST.SP.800-171r3
3.12.2 – "Develop and implement plans of action … to correct deficiencies and reduce or eliminate vulnerabilities." NIST.SP.800-171r2	**03.12.02 Plan of Action and Milestones** – Adds explicit update triggers: findings from **security assessments, audits/reviews, and continuous monitoring**. NIST.SP.800-171r3	Substantively similar, but Rev 3 makes update inputs explicit (audits/reviews, continuous monitoring) and ties POA&M operation more clearly to assessment/monitoring outcomes. NIST.SP.800-171r3
3.12.3 – "Monitor security controls on an ongoing basis to	**03.12.03 Continuous Monitoring** – "Develop and implement a **system-level continuous monitoring strategy** that includes	Rev 3 elevates from activity ("monitor controls") to a **strategy**, and couples **ongoing monitoring** with **recurring**

Rev 2 control (verbatim gist)	Rev 3 control (verbatim gist)	Explain the difference
ensure continued effectiveness." NIST.SP.800-171r2	ongoing monitoring and security assessments." NIST.SP.800-171r3	**assessments**; reinforces risk-driven frequency. NIST.SP.800-171r3
3.12.4 – "Develop, document, and periodically update **system security plans** (SSP) …" NIST.SP.800-171r2	**03.15.02 System Security Plan (Planning family)** – Relocated; adds required SSP contents (components, info types, threats, environment, roles), **review/update ODP**, and to **protect the SSP from unauthorized disclosure**. NIST.SP.800-171r3	**Relocated** out of CA to **Planning** and **expanded** (additional specifics + protection of SSP). Rev 3 also notes 03.12.04 "Withdrawn – incorporated into 03.15.02." NIST.SP.800-171r3
—	**03.12.04 Withdrawn** – "Incorporated into 03.15.02." NIST.SP.800-171r3	Not a live requirement; pointer confirming the SSP move to 03.15.02.
—	**03.12.05 Information Exchange** – Approve/manage **CUI exchanges between systems** via formal agreements (e.g., ISA/IEA/MOU-A/SLA/NDA); **document interfaces & responsibilities**; **review/update [ODP frequency]**. NIST.SP.800-171r3	**New in Rev 3**; brings **CA-03 (Information Exchange)** into scope for CUI, which Rev 2 had tailored out (CA-3 was NFO in r2). NIST.SP.800-171r2

Verification note: Rev 2 §3.12 (Security Assessment) lists exactly 3.12.1–3.12.4.

NIST.SP.800-171r2

Rev 3 §3.12 (Security Assessment and Monitoring) lists 03.12.01–03.12.05 with 03.12.04 marked "Withdrawn" and the SSP requirement present in **03.15.02** under Planning.

Delta Statement — What's New and Different in Rev 3 (CA family)

- **Family name & emphasis:** Renamed to **Security Assessment and Monitoring**, signaling a tighter coupling of assessment and ongoing monitoring.

NIST.SP.800-171r3

- **Assessment focus shift:** From assessing **controls** (r2 3.12.1) to assessing **security requirements** and the **environment of operation** (r3 03.12.01), with an **ODP** to set assessment frequency.
- **POA&M operation:** Explicitly requires updates from **assessments, audits/reviews, and continuous monitoring** (03.12.02).

NIST.SP.800-171r3

- **Continuous monitoring matured:** Requires a **system-level continuous monitoring strategy** that includes **ongoing monitoring and security assessments** (03.12.03).

NIST.SP.800-171r3

- **SSP relocation and expansion:** The **System Security Plan** moves from CA to **Planning (03.15.02)**, adds detailed SSP content and requires **protecting the SSP** from unauthorized disclosure; 03.12.04 in CA is **Withdrawn** and points to 03.15.02.
- **New requirement: 03.12.05 Information Exchange** (formal agreements for CUI exchanges, documentation, and periodic review) is **added** in Rev 3; Rev 2 had tailored CA-3 out.
- **Editorial/structural:** Rev 3 **eliminates "basic vs. derived"** labels and introduces **ODPs** broadly to tune frequency/selection values.

NIST.SP.800-171r3

Conflicts

No textual contradictions between the editions for this family were found; changes are **relocations, scope clarifications, and additions** (not reversals).

Gaps (typical deltas implementers need to address)

- **Set ODPs** for assessment/monitoring (e.g., **03.12.01 frequency**, **03.12.05 agreement types & review frequency**).

NIST.SP.800-171r3

- **Elevate monitoring** to a **documented system-level strategy** (not just activity).

NIST.SP.800-171r3

- **Formalize information exchange** via approved agreements and **document interfaces/responsibilities**.

NIST.SP.800-171r3

- **Update SSP** to Rev 3's content list and **protect it from unauthorized disclosure** (now in 03.15.02).

NIST.SP.800-171r3

Recommendations

1. **Define ODP values** now (assessment cadence for 03.12.01; agreement selections and review cadence for 03.12.05). Record them in policy/SSP.

NIST.SP.800-171r3

2. **Publish a Continuous Monitoring Strategy** that explicitly includes ongoing monitoring and recurring assessments; align inputs/outputs with POA&M updates.

NIST.SP.800-171r3

3. **Inventory all CUI exchanges** (internal & external); put **IEA/ISA/MOU-A/SLA/NDA** in place; capture **interfaces, security requirements, and responsibilities**.

NIST.SP.800-171r3

4. **Refactor the SSP** to meet **03.15.02** content and **implement SSP protection controls** (access control/handling).

NIST.SP.800-171r3

5. **Map old → new** in your compliance matrix (3.12.x → 03.12.0x / 03.15.02) to demonstrate continuity for assessors.

Brief — SC: System and Communications Protection (Rev 2 vs Rev 3)
I indexed both PDFs you provided (NIST SP 800-171 Rev 2 and Rev 3) and built a control-by-control crosswalk for the **System and Communications Protection** family. Every SC requirement from **Rev 2 (3.13.1–3.13.16)** and every enumerated SC item from **Rev 3 (03.13.01–03.13.16)** is covered below, with explicit notes for items that were consolidated, moved, or

Rev 2 (3.13.x)	Rev 3 (03.13.xx)	Explain the Difference
3.13.1 Monitor, control, and protect communications at external and key internal boundaries. NIST.SP.800-171r2	**03.13.01** Boundary Protection (a–c): monitor/control at external and key internal **managed interfaces**; require DMZs for publicly accessible components; **connect to external systems only through managed interfaces**. NIST.SP.800-171r3	Rev 3 **expands** scope by naming managed interfaces and **adds** the "connect only through managed interfaces" clause. Rev 2's DMZ requirement (3.13.5) is **incorporated** into 03.13.01. NIST.SP.800-171r3
3.13.2 Apply security engineering principles. NIST.SP.800-171r2	**Moved to SA**: **03.16.01** (System & Services Acquisition – Security & Privacy Engineering Principles). NIST.SP.800-171r3	In Rev 2, this lived in SC because SA wasn't fully included; in Rev 3 it's **re-categorized** under SA (not SC). NIST.SP.800-171r3
3.13.3 Separate user functionality from system management functionality. NIST.SP.800-171r2	**03.13.03 – Withdrawn**; addressed by **03.01.01–03.01.07** (Access Control family). NIST.SP.800-171r3	Rev 3 treats this separation via **Access Control** requirements (account management, access enforcement, information-flow, least privilege, etc.). NIST.SP.800-171r3

Rev 2 (3.13.x)	Rev 3 (03.13.xx)	Explain the Difference
3.13.4 Prevent unauthorized/unintended info transfer via shared system resources. NIST.SP.800-171r2	**03.13.04** Information in Shared System Resources. NIST.SP.800-171r3	Substantively **retained**. Terminology and discussion are carried over. NIST.SP.800-171r3
3.13.5 Implement DMZ subnetworks for publicly accessible components. NIST.SP.800-171r2	**03.13.05 – Withdrawn; incorporated into 03.13.01.** NIST.SP.800-171r3	The DMZ concept **moves into** 03.13.01(b). Rev 3 no longer lists a separate control for it. NIST.SP.800-171r3
3.13.6 Deny network traffic by default; allow by exception. NIST.SP.800-171r3	**03.13.06** Deny by Default – Allow by Exception. NIST.SP.800-171r3	**Retained** with equivalent intent; Rev 3 clarifies it applies at the boundary and identified internal points. NIST.SP.800-171r3
3.13.7 Prevent split tunneling for remote devices. NIST.SP.800-171r3	**03.13.07 – Withdrawn**; addressed by **03.01.12** (Remote Access) and others. NIST.SP.800-171r3	Split tunneling prohibitions are now handled via **Remote Access** policy/controls in the AC family (03.01.12). NIST.SP.800-171r3
3.13.8 Implement crypto to protect CUI **in transit** (or use alternative physical safeguards). NIST.SP.800-171r3	**03.13.08 Transmission and Storage Confidentiality** (crypto for CUI **in transit and at rest**). NIST.SP.800-171r3	Rev 3 **consolidates and expands**: transit + storage protection are handled **together** under 03.13.08 (see also 03.13.16 status below). NIST.SP.800-171r3

Rev 2 (3.13.x)	Rev 3 (03.13.xx)	Explain the Difference
3.13.9 Terminate network connections at session end or after inactivity. NIST.SP.800-171r2	**03.13.09** Network Disconnect (includes an **ODP** for inactivity time). NIST.SP.800-171r3	**Retained**, with an organization-defined inactivity period parameter added in Rev 3. NIST.SP.800-171r3
3.13.10 Establish/manage crypto keys. NIST.SP.800-171r2	**03.13.10** Cryptographic Key Establishment and Management (adds explicit **ODP** for key lifecycle requirements). NIST.SP.800-171r3	**Retained**, with clearer key-management expectations and references in Rev 3. NIST.SP.800-171r3
3.13.11 Employ FIPS-validated cryptography to protect CUI. NIST.SP.800-171r2	**03.13.11** Cryptographic Protection: implement **organization-defined types** of cryptography; **FIPS-validated cryptography is recommended**. NIST.SP.800-171r3	Wording **shifts** from "employ FIPS-validated" in Rev 2 to Rev 3's ODP-based specification with FIPS **recommended** (not mandated) in the base text. NIST.SP.800-171r3
3.13.12 Prohibit remote activation of collaborative computing devices; indicate device in use. NIST.SP.800-171r2	**03.13.12** Collaborative Computing Devices and Applications (adds ODP for **exceptions** where remote activation is allowed). NIST.SP.800-171r3	**Retained**, with an **allowable-exceptions** mechanism defined by the organization in Rev 3. NIST.SP.800-171r3
3.13.13 Control and monitor use of mobile code. NIST.SP.800-171r2	**03.13.13** Mobile Code (explicitly requires **defining acceptable mobile code/technologies**, then authorizing/monitoring/controlling). NIST.SP.800-171r3	**Strengthened**: Rev 3 adds an explicit "**define acceptable mobile code**" step before authorize/monitor/control. NIST.SP.800-171r3

Rev 2 (3.13.x)	Rev 3 (03.13.xx)	Explain the Difference
3.13.14 Control and monitor use of **VoIP**. NIST.SP.800-171r2	**03.13.14 – Withdrawn** (technology-specific). NIST.SP.800-171r3	Rev 3 **removes** technology-specific VoIP control.
3.13.15 Protect **session authenticity**. NIST.SP.800-171r2	**03.13.15** Session Authenticity (same concept; discussion updated). NIST.SP.800-171r3	**Retained**; Rev 3 clarifies adversary-in-the-middle, session hijacking, etc. NIST.SP.800-171r3
3.13.16 Protect confidentiality of CUI **at rest**. NIST.SP.800-171r2	**03.13.16 – Withdrawn**; **incorporated into 03.13.08** (Transmission and Storage Confidentiality).	Rev 3 **merges** "at rest" into 03.13.08, creating a single transit+storage requirement. NIST.SP.800-171r3
—	**03.13.02 – Withdrawn** (recategorized as **NCO** / out-of-scope). NIST.SP.800-171r3	This numbered slot exists in Rev 3 but is **not a requirement**; Table 20 shows some SC controls (e.g., SC-02) tailored **out** for CUI. NIST.SP.800-171r3

withdrawn. Citations point directly to the relevant passages in each document.

Evidence Table — Crosswalk (Rev 2 ⇄ Rev 3, SC Family)

Verification note: The mappings above account for **all Rev 2 SC controls (3.13.1–3.13.16)** and every **Rev 3 SC enumeration (03.13.01–03.13.16)**, including items that are **withdrawn** or **moved** to other families (e.g., **03.16.01** in SA, **03.01.12** in AC). Evidence is cited inline to the two PDFs you provided.

Delta Statement — What's new/different in Rev 3 (SC)

- **Boundary Protection broadened & consolidated.** DMZ/subnetworking from Rev 2 (3.13.5) is folded into **03.13.01** and Rev 3 adds an explicit rule to **connect only via managed interfaces**.
- **Transit + Storage combined.** Rev 2's **in-transit** (3.13.8) and **at-rest** (3.13.16) become **03.13.08 Transmission and Storage Confidentiality**; 03.13.16 is **withdrawn**.
- **Cryptography language changes.** Rev 2 required **FIPS-validated cryptography**; Rev 3's **03.13.11** uses an **ODP** to specify crypto types and states **FIPS-validated is recommended**.

NIST.SP.800-171r3

- **Collaborative tools clarified.** Rev 3 keeps prohibiting remote activation but allows **organization-defined exceptions** (ODP) and updates examples/devices.

NIST.SP.800-171r3

- **Mobile code strengthened.** Rev 3 requires you to **define acceptable mobile code** then authorize/monitor/control use.

NIST.SP.800-171r3

- **VoIP control removed.** Technology-specific VoIP requirement (**3.13.14**) is **withdrawn** as too specific.

NIST.SP.800-171r3

- **Split tunneling repositioned.** Explicit SC prohibition is **withdrawn**; now addressed via **Remote Access** controls (e.g., **03.01.12**).
- **Engineering principles moved.** Rev 2's security engineering in SC shifts to **SA** in Rev 3 (**03.16.01**).

NIST.SP.800-171r3

Conflicts (or Potential Misreads)

- **"FIPS-validated crypto" vs "recommended."** Teams accustomed to Rev 2 may assume Rev 3 **loosens** the requirement. The **base text** now says "recommended," governed by **organization-defined** parameters in 03.13.11. Ensure your overlays/contracts don't still **mandate** FIPS-validated modules.

NIST.SP.800-171r3

- **Where did split tunneling go?** It's not "missing"—it's **handled under AC** remote access (03.01.12), per Rev 3's withdrawal note for 03.13.07.
- **DMZ placement.** Some readers may look for a discrete DMZ control. In Rev 3, it's **inside** 03.13.01(b), and **03.13.05** is marked withdrawn/merged.

Gaps to Close During Adoption

- **Define ODP values** now required in SC: inactivity timeout for **03.13.09**; crypto types for **03.13.11**; any permitted exceptions for **03.13.12**.
- **Update architecture documentation** to reflect **managed interfaces** and the consolidated **boundary** expectations in **03.13.01**.

NIST.SP.800-171r3

- **Re-site controls** moved out of SC (e.g., engineering principles to **03.16.01/SA**, split tunneling into **03.01.12/AC**).

Recommendations

1. **Set the ODPs**:
    - **03.13.09** inactivity period (network disconnect).

NIST.SP.800-171r3

    - **03.13.11** cryptography types (document whether you'll require **FIPS-validated** modules organization-wide).

NIST.SP.800-171r3

    - **03.13.12** list any **allowed exceptions** for remote activation of collaborative devices, with risk rationale.

NIST.SP.800-171r3

2. **Refresh boundary architecture** and SSP diagrams to show **managed interfaces, DMZ placement, and external connections through managed interfaces only** per **03.13.01(a–c)**.

NIST.SP.800-171r3

3. **Revise policies**: move security engineering content to **SA (03.16.01)** and remote-access/split-tunneling handling to **AC (03.01.12)** so your control narrative aligns with Rev 3's families.
4. **Harden crypto posture**: even though Rev 3 phrases FIPS as "recommended," keep (or adopt) **FIPS-validated** cryptography where feasible and record that decision in your ODPs and SSP.

NIST.SP.800-171r3

5. **Train implementers and assessors** on the **merged** transit+storage confidentiality control (**03.13.08**) and the **withdrawn** tech-specific VoIP control to avoid checklist drift.

Brief (SI — System & Information Integrity)
Rev. 3 streamlines SI by collapsing separate anti-malware update/scan requirements (Rev. 2 3.14.4/.5) into a single, more prescriptive requirement (03.14.02), adds explicit organization-defined parameters (ODPs) for patch timing and scan frequency, consolidates monitoring/unauthorized-use (Rev. 2 3.14.6/.7) under 03.14.06, and introduces a new requirement for CUI information management and retention (03.14.08). Withdrawn placeholders (03.14.04, 03.14.05, 03.14.07) document these consolidations.

Evidence Table — Crosswalk (Rev 2 ↔ Rev 3) — System & Information Integrity (SI)

Rev 2 Control	Rev 3 Control	Explain the Difference
3.14.1 – Identify, report, and correct system flaws in a timely manner. NIST.SP.800-171r2	**03.14.01 Flaw Remediation** – Identify/report/correct flaws **and** install security-relevant updates within an **ODP** time period. NIST.SP.800-171r3	Substantively aligned; Rev 3 adds an explicit, assignable **time window** to install updates (ODP 03.14.01.b). NIST.SP.800-171r3
3.14.2 – Provide protection from malicious code at designated locations. NIST.SP.800-171r2	**03.14.02 Malicious Code Protection** – Implement at entry/exit points; **update** mechanisms; **configure** to (1) run periodic + real-time scans at endpoints/entry/exit and (2) **block/quarantine** on detection. NIST.SP.800-171r3	Rev 3 merges Rev 2 **3.14.4** (updates) and **3.14.5** (scans) into a single, prescriptive control, and recognizes non-signature (heuristic/AI) detection. Scan **frequency** becomes an ODP (03.14.02.c.01).
3.14.3 – Monitor system security alerts/advisories and act. NIST.SP.800-171r2	**03.14.03 Security Alerts, Advisories, and Directives** – **Receive** external alerts/advisories/directives **and generate/disseminate** internal alerts/directives as needed. NIST.SP.800-171r3	Scope expands to include **directives** and internal dissemination (CISA/NSA/FBI sources noted). NIST.SP.800-171r3

Rev 2 Control	Rev 3 Control	Explain the Difference
3.14.4 – **Update** malicious-code protection when new releases are available. NIST.SP.800-171r2	**03.14.02 (b)** – Update malicious-code protection per CM policies; **03.14.04** labeled **Withdrawn** (incorporated into 03.14.02).	Content carried into 03.14.02; standalone Rev 2 item removed; 03.14.04 documents consolidation. NIST.SP.800-171r3
3.14.5 – Perform periodic scans and real-time scans of external files. NIST.SP.800-171r2	**03.14.02 (c.1–c.2)** – Requires periodic + real-time scans **and** mandates **block/quarantine/mitigation** on detection; **03.14.05** marked **Withdrawn** (addressed by 03.14.02).	Rev 3 elevates scanning into explicit configuration outcomes; standalone Rev 2 item removed and tracked as withdrawn. NIST.SP.800-171r3
3.14.6 – Monitor systems (incl. inbound/outbound traffic) to detect attacks/indicators. NIST.SP.800-171r2	**03.14.06 System Monitoring** – Monitor for **attacks, indicators, and unauthorized connections**; **identify unauthorized use**; monitor inbound/outbound for unusual or unauthorized activity. NIST.SP.800-171r3	Consolidates and broadens monitoring; explicitly adds **unauthorized connections** and folds "unauthorized use" into this control. (Rev 3 Table 21 shows SI-04 → 03.14.06.) NIST.SP.800-171r3
3.14.7 – Identify unauthorized use of organizational systems. NIST.SP.800-171r2	**03.14.06 (b)** – "Identify unauthorized use" within system monitoring; **03.14.07** is **Withdrawn** (incorporated into 03.14.06).	Requirement retained but **embedded** in 03.14.06; 03.14.07 records the consolidation. NIST.SP.800-171r3
—	**03.14.04 Withdrawn** – Incorporated into 03.14.02. NIST.SP.800-171r3	Structural note only; no direct Rev 2 counterpart

Rev 2 Control	Rev 3 Control	Explain the Difference
		beyond 3.14.4 content now in 03.14.02. NIST.SP.800-171r3
—	**03.14.05 Withdrawn** – Addressed by 03.14.02. NIST.SP.800-171r3	Structural note; Rev 2 3.14.5 content is captured under 03.14.02. NIST.SP.800-171r3
—	**03.14.07 Withdrawn** – Incorporated into 03.14.06. NIST.SP.800-171r3	Structural note; Rev 2 3.14.7 is now part of 03.14.06. NIST.SP.800-171r3
— (Rev 2 did **not** include SI-12; marked **FED** in Appendix E Table E-17) NIST.SP.800-171r2	**03.14.08 Information Management and Retention** – Manage/retain CUI and CUI outputs per laws, EOs, directives, regs, policies, standards, guidelines, and operational requirements. NIST.SP.800-171r3	**New in Rev 3.** Rev 2 tailored SI-12 out as uniquely federal; Rev 3 adds a CUI-focused requirement (Table 21: SI-12 → 03.14.08). NIST.SP.800-171r3

QC coverage check: Rev 2 SI has **7** requirements (3.14.1–3.14.7) — all mapped above. Rev 3 SI enumerates **8** items, of which **5 are active** (03.14.01, .02, .03, .06, .08) and **3 are Withdrawn** (.04, .05, .07) — all represented above.

Delta Statement (what's new/different in Rev 3 — SI)

- **Single, prescriptive anti-malware control:** Rev 3 **combines** Rev 2's update (**3.14.4**) and scanning (**3.14.5**) into **03.14.02**, which now mandates **periodic and real-time scans**, and explicit **block/quarantine/mitigation** actions; older fragments are flagged as **Withdrawn** (03.14.04/.05). ODP adds scan **frequency**.

- **Patch timing made explicit: 03.14.01** introduces an **ODP** to define the required **time period** for installing security-relevant updates — raising specificity compared to Rev 2's "timely manner."
- **Broader alerting posture: 03.14.03** adds **internal** generation/dissemination of alerts **and directives**, whereas Rev 2 emphasized monitoring external advisories and taking action.
- **Monitoring consolidation & expansion: 03.14.06** unifies Rev 2 **3.14.6** and **3.14.7** and explicitly requires detecting **unauthorized connections** as well as attacks/indicators and unauthorized use; **03.14.07** is marked **Withdrawn** to record the merge.
- **New requirement: 03.14.08 Information Management and Retention** requires managing/retaining **CUI** and outputs per applicable mandates — new to Rev 3; Rev 2 treated SI-12 as uniquely federal and did not include it. (Rev 3 Appendix C Table 21 maps **SI-12 → 03.14.08**.)
- **Meta-changes affecting SI overall:** Rev 3 **eliminates basic/derived labels**, **adds ODPs**, and **groups/removes redundancies** (e.g., the Withdrawn markers), improving implementability and assessment clarity. (See Rev 3 Change Log.)

NIST.SP.800-171r3

Conflicts (interpretation pitfalls to watch)

- **"Withdrawn" ≠ removed capability:** 03.14.04/.05/.07 are labels documenting consolidation; their **substance** lives in 03.14.02 and 03.14.06. Treating them as "not required" can leave gaps.
- **Rev 2 vs Rev 3 wording drift:** Rev 3's prescriptive phrasing (e.g., explicit blocking/quarantining) can be stricter than legacy Rev 2 interpretations; relying on Rev 2 language alone under-scopes controls.

NIST.SP.800-171r3

Gaps (implementation decisions you must fill)

- **Set ODP values:**
    - Patch/install window for **03.14.01.b**.

    - System-wide scan **frequency** for **03.14.02.c.01**.
      These values are required to “complete” the requirement text.

NIST.SP.800-171r3

- **Document CUI retention rules:** Define authoritative sources and retention schedules to meet **03.14.08** (coordination with records owners & contracts).

NIST.SP.800-171r3

- **Monitoring scope:** Ensure tooling and procedures cover **unauthorized connections** (explicit in **03.14.06**), not just attack indicators.

NIST.SP.800-171r3

Recommendations

1. **Update policies/SSP:** Insert Rev 3 ODPs (patch window; scan cadence) and the explicit **block/quarantine** response in your anti-malware standard (maps to **03.14.01/.02**).
2. **Consolidate procedures:** Merge legacy Rev 2 malware update/scan SOPs into one Rev 3 **03.14.02** procedure with tuning for endpoints and gateways.

NIST.SP.800-171r3

3. **Enhance monitoring use-cases:** Add detections for **unauthorized connections** and **unauthorized use**, and validate inbound/outbound analytics align with **03.14.06**.

NIST.SP.800-171r3

4. **Stand up a CUI retention playbook:** Implement **03.14.08** by mapping CUI types to retention schedules and purge workflows; align with contract/recordkeeping requirements.

NIST.SP.800-171r3

5. **Rev 2→Rev 3 traceability:** Keep this crosswalk as evidence for audit; cite Rev 3 Appendix C **Table 21** (SI mapping) in your package to show source-control lineage.

NIST.SP.800-171r3

Brief Planning (PL) — Rev 2 vs Rev 3 Crosswalk

- Rev 3 **introduces a Planning (PL) family** with three requirements: Policy & Procedures, System Security Plan, and Rules of Behavior.

NIST.SP.800-171r3

- Rev 2 **did not include a Planning family**; however, its **system security plan** requirement lived under *Security Assessment* (3.12.4).
- Crosswalk outcome:
    - **03.15.02 (Rev 3)** ↔ **3.12.4 (Rev 2)** (direct lineage, expanded).
    - **03.15.01** and **03.15.03** are **new in Rev 3** (no Rev 2 equivalents; policy/procedure and rules-of-behavior topics were tailored out).

Evidence Table (Planning Family Crosswalk)

Rev 2 (ID • Title)	**Rev 3 (ID • Title)**	**Explain the Difference**
(no PL family in scope)	**03.15.01 • Policy and Procedures**	New requirement in Rev 3 to develop, disseminate, review and update policies & procedures for protecting CUI across all families. Rev 2 tailored "policy and procedures" controls out of scope (e.g., CM-1, RA-1 marked NFO) and had **no Planning family**.
3.12.4 • System Security Plans *(in Security Assessment family)*	**03.15.02 • System Security Plan**	Rev 3 relocates and **expands** SSP content: explicitly enumerates components, information types, threats, environment/dependencies, requirements overview, safeguards, roles, and other relevant info; adds **review/update frequency (ODP)** and **protect SSP from unauthorized disclosure**. Rev 2 required SSP describing boundaries, environment, implementation, and interconnections—but with less prescriptive detail and no explicit protection clause.

Rev 2 (ID • Title)	Rev 3 (ID • Title)	Explain the Difference
(no explicit equivalent; PS-6 "Access Agreements" was tailored out as NFO)	**03.15.03 • Rules of Behavior**	**New** in Rev 3: establish, disseminate, obtain **acknowledgment** of rules of behavior before authorizing access; review/update at an ODP-defined frequency. Rev 2 had **no CUI requirement** for access agreements or rules of behavior (PS-6 = NFO).

Verification of completeness: Rev 3's **Table 14** lists exactly three PL requirements (PL-01 → 03.15.01, PL-02 → 03.15.02, PL-04 → 03.15.03); all others in the PL family are FED/NCO and not requirements. All three are included above. Rev 2 Chapter Two confirms Planning was out of scope, with the *exception* of the SSP requirement placed under Security Assessment (3.12.4).

Delta Statement (what's new/different in Rev 3 — Planning)

- **New family**: Planning (PL) now exists with three requirements.

NIST.SP.800-171r3

- **Policies & procedures**: Organizations must formalize CUI policies and procedures and set an **ODP-defined** review cadence (03.15.01).

NIST.SP.800-171r3

- **System Security Plan (SSP)**: Requirement **moved** from Rev 2's 3.12.4 to **03.15.02**, and **expanded** with explicit content elements; adds protection of the SSP and ODP-driven review frequency.
- **Rules of Behavior**: **New** Rev 3 requirement (03.15.03) including **signed acknowledgment** prior to granting access and periodic updates; Rev 2 had no equivalent CUI requirement.

Conflicts

- **None found** between Rev 2 and Rev 3 language; the change is **structural (relocation)** and **scope-expansion**. SSP expectations in Rev 3 subsume and clarify Rev 2's 3.12.4.

Gaps (typical when migrating from Rev 2 → Rev 3)

- **Missing enterprise CUI policies/procedures** (03.15.01) if you only implemented technical controls under Rev 2.

NIST.SP.800-171r3

- **Rules-of-behavior program** (acknowledgments, periodic review) often absent in Rev 2 implementations because PS-6 and PL-4 were out of scope.
- **SSP depth & protection**: SSPs may lack Rev 3's enumerated content and may not be explicitly safeguarded or reviewed at an ODP-defined interval.

NIST.SP.800-171r3

Recommendations

1. **Stand up a PL policy stack**: Issue or update CUI security **policies and procedures** for each family and set an **ODP** review frequency (e.g., annually). Map each policy to the corresponding Rev 3 family.

NIST.SP.800-171r3

2. **Modernize the SSP** to Rev 3: Ensure the SSP covers **all eight elements** listed in 03.15.02; add a protection/handling statement; define and document the **review/update cadence** (ODP).

NIST.SP.800-171r3

3. **Implement Rules of Behavior**: Draft role-specific rules (general vs. privileged users), require **signed acknowledgments prior to access**, and schedule periodic reviews/refreshers.

NIST.SP.800-171r3

4. **Traceability**: In your crosswalk, record that Rev 2 **3.12.4 → Rev 3 03.15.02** to demonstrate continuity for assessors.

Brief — System & Services Acquisition (SA) Crosswalk (Rev 2 ↔ Rev 3)
Rev 3 introduces a dedicated **System & Services Acquisition (SA)** family with three requirements (03.16.01–03.16.03). In Rev 2 there was **no SA family**; one SA concept (security engineering principles) lived under **System & Communications Protection (SC)** as 3.13.2, and "external systems" obligations appeared in **Access Control (AC)** as 3.1.20. Rev 3 also adds an explicit requirement to address **unsupported components**. Coverage below verifies **all SA requirements in Rev 3** and lines them up with Rev 2 where possible.

NIST.SP.800-171r3

NIST.SP.800-171r3

Evidence Table — SA Family Crosswalk

Rev 2 requirement(s)	Rev 3 requirement(s)	Explain the difference
No separate SA family in Rev 2. Rev 2 explicitly excluded the SA family; SA-8 was grouped under SC. (Appendix E, Table E-15, note.)	**SA family exists in Rev 3** (Table 1 lists **System and Services Acquisition** among the 17 families).	Structural change: Rev 3 creates a standalone SA family; Rev 2 only referenced SA concepts indirectly. NIST.SP.800-171r2 NIST.SP.800-171r3
3.13.2 *Employ architectural designs, software development techniques, and systems engineering principles* … (SC family)	**03.16.01 Security Engineering Principles** (SA-08 source)	Substantively aligned but **relocated** from SC→SA. Rev 3 adds an **ODP** to specify which engineering principles the org will use, increasing clarity and auditability. NIST.SP.800-171r2 NIST.SP.800-171r3
— **No direct equivalent in Rev 2** (SA-22 not present and no explicit replacement/mitigation duty)	**03.16.02 Unsupported System Components** (SA-22 source)	**New in Rev 3.** Requires replacing unsupported components **or** implementing mitigations/alternate support; not mandated in Rev 2. NIST.SP.800-171r3

Rev 2 requirement(s)	Rev 3 requirement(s)	Explain the difference
		NIST.SP.800-171r2
3.1.20 *Verify and control/limit connections to and use of external systems* (AC family)	**03.16.03 External System Services** (SA-09 source). Rev 3 explicitly notes relation to **03.01.20**.	Rev 3 goes **beyond** Rev 2's "verify & control" by requiring: (a) **provider compliance** with defined security requirements (**ODP**), (b) **documented roles/responsibilities** (shared with providers), and (c) **ongoing monitoring** of provider compliance; introduces explicit **SLA/contract** expectations. NIST.SP.800-171r2 NIST.SP.800-171r3

Verification notes: Rev 3 SA family contains exactly **03.16.01, 03.16.02, 03.16.03** (Section 3.16). Table 19 in Rev 3 shows SA-08→03.16.01, SA-22→03.16.02, SA-09→03.16.03. Rev 2 Appendix E Table E-15 confirms SA family not included and lists SA-8 grouped elsewhere.

NIST.SP.800-171r3

NIST.SP.800-171r3

Delta Statement — What's new/different in Rev 3 (SA)

1. **New SA family created.** Rev 3 formalizes **System & Services Acquisition** as its own family; Rev 2 had **no SA family** (SA-8 was embedded under SC).

NIST.SP.800-171r2

NIST.SP.800-171r3

2. **Relocation & clarity:** Rev 2 **3.13.2** (SC) becomes **03.16.01** (SA). Rev 3 adds an **organization-defined parameter (ODP)** to name the engineering principles used, improving implementability and assessment.

NIST.SP.800-171r3

3. **Unsupported components now required:** Rev 3 adds **03.16.02**, obligating replacement or documented mitigations/alternate support for **unsupported system components**—not explicit in Rev 2.

NIST.SP.800-171r3

4. **External services strengthened:** Rev 3 **03.16.03** requires **contractually defined security requirements (ODP), documented shared responsibilities, and continuous monitoring** of **external service providers**; Rev 2 **3.1.20** focused on verifying/controlling use of external systems.

NIST.SP.800-171r3

NIST.SP.800-171r2

5. **Traceability to 800-53B tailoring:** Rev 3's Appendix/Table mapping shows the SA controls (SA-08, SA-09, SA-22) and where they land in 03.16.xx, aiding objective crosswalks.

NIST.SP.800-171r3

Conflicts

- **No direct contradictions** found. Differences are **scope/placement** changes (SC→SA) and **new obligations** (unsupported components; provider compliance + monitoring). Evidence: Rev 2 exclusion of SA family and Rev 3's explicit SA section and tables.

NIST.SP.800-171r2

NIST.SP.800-171r3

Gaps (from Rev 2 → Rev 3)

- **Unsupported components**: No explicit Rev 2 requirement; **03.16.02** fills that gap.

NIST.SP.800-171r3

- **Provider governance**: Rev 2's **3.1.20** stops at verifying/controlling externals; Rev 3 **03.16.03** requires **defined security requirements, roles/responsibilities, and ongoing monitoring** (plus SLAs).

NIST.SP.800-171r3

NIST.SP.800-171r2

- **ODPs**: Rev 3 introduces ODPs for **03.16.01** and **03.16.03**, requiring organizations to set explicit values; this flexibility/specificity did not exist in Rev 2. (See Appendix D.)

NIST.SP.800-171r3

Recommendations

1. **Publish an SA Policy & Procurement Playbook** mapping Rev 3 SA objectives into sourcing: pre-award security requirements, evaluation criteria, and **contract clauses/SLA language** obligating providers to meet **03.16.03** (including reporting, metrics, and audit/inspection rights).

NIST.SP.800-171r3

2. **Define ODPs**:
    - For **03.16.01**, adopt a concrete set of **systems security engineering principles** (e.g., from SP 800-160) and record them as the SA ODP.
    - For **03.16.03**, define the **security requirements** providers must meet (controls in scope, evidence cadence, response times). (Appendix D lists the ODP fields.)

NIST.SP.800-171r3

3. **Unsupported components program** (for **03.16.02**): maintain an asset inventory with **support status**, establish **replacement timelines**, and for exceptions, document **mitigations** (isolation, compensating controls, alternative support contracts) and **risk acceptance**.

NIST.SP.800-171r3

4. **Tie to information-exchange governance**: align SA contracting artifacts with **03.12.05 Information Exchange** (use ISAs/SLAs/MOUs to document interfaces, security requirements, roles).

NIST.SP.800-171r3

5. **Continuous provider monitoring**: operationalize **03.16.03(c)** with a vendor-risk cadence (evidence reviews, scan/exposure attestation, incident notice windows) and integrate with security monitoring and assessments.

NIST.SP.800-171r3

Brief — Supply Chain Risk Management (SR) crosswalk (Rev 2 → Rev 3)
Rev 2 has no dedicated "Supply Chain Risk Management" family. Rev 3 introduces a full SR family (03.17.*) and also binds SR policy into the new Planning family (03.15.01) while making supplier review part of Risk Assessment (03.11.01). The table below lines up every SR-relevant Rev 3 requirement with its Rev 2 counterpart (or closest analog) and explains the deltas, with paragraph-level citations to the attached PDFs.

NIST.SP.800-171r3

Crosswalk Table — Supply Chain Risk Management (SR)

Rev 2 (SP 800-171r2)	Rev 3 (SP 800-171r3)	Explain the difference
No SR family / no family-level Policy & Procedures requirement in scope. Rev 2 tailored out most family "policy & procedures" controls as **NFO** (not required) (e.g., SA-1, SC-1). NIST.SP.800-171r2	**03.15.01 Policy & Procedures** — organization establishes and maintains policies & procedures for each requirement family (explicitly includes **SR-01**). NIST.SP.800-171r3	Rev 3 makes family-level policy & procedures mandatory and explicitly ties them to SR; Rev 2 did not require these at the family level. NIST.SP.800-171r2 NIST.SP.800-171r3
Closest analog: 3.12.4 System Security Plan (SSP) — develop, document, and update SSP; not supply-chain-specific. NIST.SP.800-171r2	**03.17.01 Supply Chain Risk Management Plan** — develop, maintain, and protect a **SCRM plan**; may be standalone or integrated into the SSP. NIST.SP.800-171r3	Rev 3 requires a dedicated, reviewable SCRM plan; Rev 2 only required a general SSP with no explicit SCRM planning elements. NIST.SP.800-171r2 NIST.SP.800-171r3
No direct control. Closest analogs: 3.1.20 verify and control/limit connections to external systems; **3.13.2** apply security engineering principles	**03.17.02 Acquisition Strategies, Tools, and Methods** — implement procurement and contracting strategies to	Rev 3 adds concrete acquisition-time SCRM methods (e.g., tamper-evident packaging, trusted

Rev 2 (SP 800-171r2)	Rev 3 (SP 800-171r3)	Explain the difference
— both tangential to acquisition-stage risk. NIST.SP.800-171r2 NIST.SP.800-171r2	identify, protect against, and mitigate supply chain risks. NIST.SP.800-171r3	distribution); Rev 2 had no acquisition-focused SCRM requirement. NIST.SP.800-171r3
No direct control. Closest analogs: 3.1.20 external systems; **3.13.2** security engineering — general practices that can support provenance/configuration, but not a formal SR process. NIST.SP.800-171r2 NIST.SP.800-171r2	**03.17.03 Supply Chain Requirements & Processes** — establish processes to identify/address weaknesses in supply-chain elements and enforce **organization-defined** SR security requirements. NIST.SP.800-171r3	Rev 3 mandates formal SR processes and enforcement of org-defined SR controls; Rev 2 had only scattered, indirect coverage. NIST.SP.800-171r3
3.11.1 Risk Assessment — periodic RA; considers risk from external parties but does not explicitly call out supplier/contractor SCRM. NIST.SP.800-171r2	**03.11.01 Risk Assessment** — *explicitly includes supply-chain-related risks associated with suppliers/contractors and the systems/services they provide* (SR-06 mapping). NIST.SP.800-171r3	Rev 3 strengthens RA to explicitly include supplier assessments and supply-chain risk; Rev 2's RA was more general and implicit. NIST.SP.800-171r2 NIST.SP.800-171r3

Verification note: The SR family coverage in Rev 3 equals SR-01→**03.15.01**, SR-02→**03.17.01**, SR-03→**03.17.03**, SR-05→**03.17.02**, SR-06→**03.11.01** (other SR controls are tailored out as NCO/ORC).

NIST.SP.800-171r3

Delta Statement — What's new/different in Rev 3 (SR)

- **Dedicated SCRM family and plan.** Rev 3 adds **03.17.01–03.17.03**, requiring a **SCRM plan**, acquisition-time SCRM controls, and enforceable supply-chain processes — none of which existed as explicit requirements in Rev 2.

NIST.SP.800-171r3

NIST.SP.800-171r3

- **Supplier risk is explicit in RA.** Rev 3's **03.11.01** requires supply-chain risk to be assessed (including supplier/contractor-provided components/services); Rev 2's **3.11.1** discussed external parties generally but did not explicitly scope supplier SCRM.

NIST.SP.800-171r3

NIST.SP.800-171r2

- **Family-level policies now required.** Rev 3 mandates **03.15.01** policies & procedures for each family (including SR-01); Rev 2 tailored out family P&P (e.g., SA-1, SC-1 marked NFO).

NIST.SP.800-171r3

NIST.SP.800-171r2

- **Related but outside SR:** Rev 3 introduces **03.16.03 External System Services** (manage/monitor external service providers), whereas Rev 2 treated SA-9 External System Services as not required (NFO). This materially tightens supply-chain oversight even though it lives in the SA family.

NIST.SP.800-171r3

NIST.SP.800-171r2

Evidence Table (key sources)

Topic	**Rev 3 source**	**Rev 2 source**
SR family coverage & mappings (SR-01/02/03/05/06)	Table 22 "Supply Chain Risk Management (SR)". NIST.SP.800-171r3	—

Topic	Rev 3 source	Rev 2 source
03.17.01 SCRM Plan (text & discussion)	§3.17.01. NIST.SP.800-171r3	Closest analog SSP §3.12.4. NIST.SP.800-171r2
03.17.02 Acquisition strategies/tools/methods	§3.17.02. NIST.SP.800-171r3	No direct control; see §3.1.20, §3.13.2 as analogs. NIST.SP.800-171r2 NIST.SP.800-171r2
03.17.03 Supply-chain requirements & processes	§3.17.03. NIST.SP.800-171r3	No direct control (analogs as above). NIST.SP.800-171r2 NIST.SP.800-171r2
03.11.01 RA (explicit supplier/supply-chain risk)	§3.11.01 (discussion). NIST.SP.800-171r3	§3.11.1 RA (external parties, not explicit SCRM). NIST.SP.800-171r2
03.15.01 Policy & Procedures (includes SR-01)	§3.15.01 (Source Controls list includes **SR-01**). NIST.SP.800-171r3	Family P&P tailored out (e.g., SA-1, SC-1 = NFO). NIST.SP.800-171r2
Related tightening outside SR: external service providers	§3.16.03 External System Services. NIST.SP.800-171r3	SA-9 External System Services = NFO (tailored out). NIST.SP.800-171r2

Conflicts / Nuances to note

- **Classification nuance:** In Rev 3, "Policy & Procedures" lives in **Planning (03.15.01)** but NIST's mapping associates it with **SR-01** for the SR family. That is expected and not a contradiction.

NIST.SP.800-171r3

NIST.SP.800-171r3

Gaps you must address to meet Rev 3 SR

- **Author and maintain a documented SCRM plan** (03.17.01) and decide where it lives (standalone vs. integrated into the SSP).

NIST.SP.800-171r3

- **Set organization-defined parameters** in **03.17.03(b)** (the SR controls you will enforce across suppliers/components/services).

NIST.SP.800-171r3

- **Make SR policy/procedures official** under 03.15.01 and align with acquisition and RA workflows.

NIST.SP.800-171r3

- **Embed SCRM into procurement** (03.17.02) and **explicitly include supplier risk in RA** (03.11.01).

NIST.SP.800-171r3

NIST.SP.800-171r3

Recommendations (actionable next steps)

1. **Draft 03.17.01 SCRM Plan** (scope, roles, supplier tiers, acceptance criteria, monitoring cadence); if integrating into the SSP, create a dedicated SCRM section and cross-reference POA&Ms.

NIST.SP.800-171r3

NIST.SP.800-171r2

2. **Update acquisition artifacts** — add SR clauses/templates (tamper-evident packaging, trusted distribution, counterfeit prohibition, disclosure obligations). Map each clause to 03.17.02.

NIST.SP.800-171r3

3. **Define and publish SR controls to enforce** for 03.17.03(b) (e.g., SBOM/attestation, secure development practices, provenance/chain-of-custody, change control for repairs).

NIST.SP.800-171r3

4. **Revise RA procedures** to include supplier/contractor risk scenarios and evidence requirements (assessments, certifications) per 03.11.01.

NIST.SP.800-171r3

5. **Adopt Planning 03.15.01** — issue SR policy & procedures and link them to acquisition and RA SOPs.

NIST.SP.800-171r3

6. **(Related)** If you rely on cloud/managed services, implement **03.16.03** controls: define shared responsibilities and monitor provider compliance.

NIST.SP.800-171r3