NIST SP 800-53 AND THE RMF.

NIST SP 800-53 Rev. 5 is a catalog of 1,014 active security and privacy controls in 20 families. SP 800-53B picks a baseline by FIPS 199 impact level, SP 800-53A says how to assess, and the SP 800-37 RMF turns them into an authorization decision: **the catalog supplies the controls; the RMF supplies the decision.**

CATALOG, NOT A CHECKLIST | IMPACT LEVEL SETS BASELINE | 20 FAMILIES, 7 RMF STEPS | ATO IS A RISK DECISION

01 THE MECHANISM

The Catalog (SP 800-53)

Rev. 5 organizes controls into 20 families, Access Control through Supply Chain Risk Management, each with base controls and enhancements. Controls are policy-, technology- and sector-neutral, and Rev. 5 made them outcome-based. **It is a menu, not a list of what to pick.** [01] [09]

Baselines and Assessment

SP 800-53B supplies three security baselines, one per FIPS 199 impact level, plus a privacy baseline applied irrespective of level, with tailoring guidance. SP 800-53A gives assessors examine, interview and test procedures. **Baselines are the starting point, not the end state.** [02] [03] [05]

The Lifecycle (SP 800-37)

The RMF runs seven steps: Prepare, Categorize, Select, Implement, Assess, Authorize and Monitor. A senior authorizing official reads the authorization package and explicitly accepts the risk or denies authorization. **OMB Circular A-130 requires federal agencies to run this process.** [04] [07]

02 THE FLOW

From Category to Controls SELECT

1. **Categorize with FIPS 199:** rate confidentiality, integrity and availability as low, moderate or high by the harm a loss would cause: limited, serious, or severe. A system takes the high water mark across its information types, so one high objective makes a high-impact system. [05] [06]
2. **Select the matching baseline:** FIPS 200 requires the low, moderate or high baseline for the impact level; SP 800-53B adds a privacy baseline where PII is processed. Low means all three objectives are low; high means any one is. Every control stays unless tailoring removes it. [06] [02]
3. **Tailor and document:** designate common controls, apply scoping considerations, choose compensating controls, set organization-defined parameters, add controls, and record it all in the security and privacy plans. An overlay packages tailoring for a community. [02] [04]

From Controls to Authorization AUTHORIZE

1. **Implement and assess:** put the planned controls in place, document the as-implemented state, then assess them with SP 800-53A procedures. Each determination statement ends satisfied or other than satisfied, and open items become the plan of action and milestones. [04] [03]
2. **Authorize on risk:** the authorizing official determines the risk, picks a response and issues an authorization to operate, a common control authorization, an authorization to use for shared or cloud services, or a denial. An ATO carries terms, conditions and a termination date. [04] [07]
3. **Monitor and reauthorize:** watch the system and its environment for change, reassess controls under the continuous monitoring strategy, report posture to management, and move to ongoing authorization when eligible. A-130 directs reauthorization on a time- or event-driven basis. [04] [07]

03 THE RMF STEPS (SP 800-37 REV. 2)

STEP	WHAT IT PRODUCES
Categorize	Prepare sets roles, risk strategy and common controls; then FIPS 199 rates impact of loss low, moderate or high.
Select	Pick the SP 800-53B baseline for that impact level, tailor it, allocate common controls, write the plans.
Implement	Put the planned controls in place and document the as-implemented state wherever it departs from the plan.
Assess	An assessor examines, interviews and tests against SP 800-53A; findings feed the plan of action and milestones.
Authorize	The authorizing official weighs the package, determines the risk and grants, conditions or denies authorization.
Monitor	Track changes, reassess controls under the monitoring strategy, report posture, and pursue ongoing authorization.

04 BASELINES COMPARED

BASELINE	SET BY IMPACT LEVEL?	WHAT IT MEANS
Privacy baseline	No	Applied irrespective of impact level where PII is processed: 96 controls and enhancements, tailored by privacy risk assessment.
Low impact	Yes	All three objectives low: a loss would have a limited adverse effect. The 5.2.0 low baseline holds 149 controls and enhancements.
Moderate impact	Yes	At least one objective moderate and none high: a serious adverse effect. The moderate baseline holds 287 controls and enhancements.
High impact	Yes	At least one objective high: a severe or catastrophic effect, up to loss of life. The largest baseline: 370 controls and enhancements.

SP 800-53 & THE RMF.

CATEGORIZE · SELECT · AUTHORIZE

05 PROGRAM OPERATIONS

Pin the release you build to. NIST patches the catalog in CPRT: Release 5.1.1 (November 7, 2023) added IA-13 and leading-zero identifiers like AC-01; Release 5.2.0 (August 27, 2025) added SA-15(13), SA-24 and SI-02(07) and left baselines untouched. Record the release your plans use. [08] [01] [02]

Categorize honestly, then tailor in writing. One high objective drives the whole system high under the high water mark, so draw authorization boundaries deliberately. Every scoping decision, compensating control and parameter value belongs in the plans, where assessors can test it. [05] [02] [04]

Use the machine-readable catalog. NIST publishes 800-53, 800-53A and 800-53B through CPRT and as OSCAL, JSON and spreadsheets, so plans and assessments can be data, not documents. The 5.2.0 OSCAL catalog holds 1,014 active controls and enhancements (300 base, 714 enhancements). [01] [09]

Treat the ATO as the start of monitoring. Write the continuous monitoring strategy during Select, not after Authorize. A-130 requires an ISCM strategy, monitoring of every selected control, and time- or event-driven reauthorization; ongoing authorization is earned by results, not declared. [07] [04]

06 CONTROL MAPPING

FEDRAMP REV5 BASELINES

FedRAMP's 2026 control reference is generated from NIST's SP 800-53 Release 5.2.0 OSCAL catalog, the same 1,014 active controls and enhancements across 20 families, and shows which FedRAMP Rev5 baseline each control belongs to, so a cloud authorization reuses this catalog rather than a separate one. [10] [09]

FISMA AND OMB A-130

SP 800-53 is mandatory for federal information systems under FISMA and A-130. Appendix I of A-130 requires agencies to categorize by FIPS 199, select controls satisfying FIPS 200 and the 800-53 baselines, complete an initial ATO before operation, and keep ISCM strategies. National security systems follow CNSS guidance. [07] [01]

FIPS 199 AND FIPS 200

FISMA's two mandatory standards: FIPS 199 (February 2004) sets the categorization scheme and the high water mark; FIPS 200 (March 2006) sets minimum requirements in 17 areas and requires the matching 800-53 baseline. Of the 20 families, 17 align with FIPS 200; PM, PT and SR address later mandates. [05] [06] [01]

NIST CSF, 800-171, CMMC

SP 800-53 notes that A-130 requires the RMF for selecting controls while Executive Order 13800 has agencies manage cybersecurity risk with the NIST Cybersecurity Framework; both are optional for nonfederal organizations. CSF 2.0 (topic 95) and CMMC 2.0 with SP 800-171 (topic 101) are neighbors, not substitutes. [01]

07 WHAT THIS DOES NOT SOLVE

Not a Checklist

The catalog never says which controls apply; **categorization, baselines and tailoring decide that.** [01] [02]

Not Technology Advice

Controls are policy-, technology- and sector-neutral by design; **how to implement them is your call.** [01]

Not a Private Mandate

Mandatory for federal information systems only; **other organizations are encouraged, not required.** [01]

Not Done at the ATO

An authorization carries conditions and a termination date; **monitoring and reauthorization continue.** [04] [07]

08 MYTHS VS. REALITY

MYTH	REALITY
"800-53 means implementing about 1,200 controls."	The 5.2.0 catalog holds 1,014 active controls and enhancements; **a system implements its tailored baseline.** [09] [02]
"Rev. 5 is frozen until Revision 6 arrives."	NIST patches it in CPRT: **Release 5.1.1 (2023) and Release 5.2.0 (2025)** changed it without a new revision. [08] [01]
"The RMF is paperwork that ends at the ATO."	Authorize is one step of seven; **A-130 requires continuous monitoring and reauthorization** after it. [04] [07]
"A moderate baseline means moderate security."	Baselines are starting points; **tailoring adds controls and stricter parameters** as risk demands. [02]
"Passing the assessment authorizes the system."	Assessors report satisfied or other than satisfied; **only the authorizing official accepts the risk**. [03] [04]

09 SPEAK THE PROGRAM — KEY TERMS

CONTROL BASELINE

The minimum set of controls for an impact level; **the starting point for tailoring**.

TAILORING

Adjusting a baseline through **scoping, compensating controls, parameters and supplements**.

OVERLAY

A specialization of baselines for a community or technology, **applied to many systems**.

HIGH WATER MARK

A system's impact per objective is **the highest value among its information types**.

AUTHORIZING OFFICIAL

The senior official who **explicitly accepts the risk** and grants or denies authorization.

ONGOING AUTHORIZATION

Time- or event-driven risk acceptance **fed by continuous monitoring results**.