



NIST SPECIAL PUBLICATION 800-53 REV 4

Security and Privacy Controls for Federal Information Systems and Organizations

The 462-page master federal control catalog — 18 security control families plus a privacy control catalog. This Executive Summary covers the catalog's structure, control families, baselines (low/moderate/high), tailoring, overlays, and the crosswalk into HIPAA Security Rule standards. Use the original NIST PDF as the source of truth for individual control wording.

NIST SP 800-53 r4

Control Catalog

Federal Baseline

Healthcare Mapping

NIST SPECIAL PUBLICATION 800-53 REVISION 4 · APRIL 2013 · CSR EXECUTIVE SUMMARY EDITION

Security and Privacy Controls for Federal Information Systems and Organizations. Authored by the NIST Joint Task Force Transformation Initiative. NIST Special Publication 800-53 Revision 4, 462 pages (April 2013, includes updates as of 01-22-2015). This Premium Edition is a CSR-branded executive summary of NIST SP 800-53 r4 — its structure, control families, baselines, and how to use it. For specific control wording (the AC-1 through PM-16 catalog itself), refer to the original 462-page NIST publication, which remains the authoritative source.

SCOPE OF THIS EDITION

NIST SP 800-53 r4 is a 462-page federal control catalog containing hundreds of individual security controls and privacy controls, each with descriptions, supplemental guidance, control enhancements, and references. Faithfully retyping every word into a polished PDF would produce a 250–350 page document of largely identical reference content to the original. This Premium Edition instead provides a CSR-branded executive overview — the document's structure, the 18 security control families, baseline selection, tailoring, and how to apply it in healthcare contexts where SP 800-53 underlies HIPAA Security Rule compliance. Keep the original NIST PDF for individual control text.

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems. Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States.

Executive Summary

NIST SP 800-53 Rev 4 provides a comprehensive catalog of security and privacy controls for federal information systems and organizations and a process for selecting controls to protect organizational operations, organizational assets, individuals, other organizations, and the nation from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.

The security controls in this publication are intended to be employed as part of a well-defined and documented information security program that supports an organization's mission and business processes. The publication provides:

- A comprehensive catalog of security controls in 18 control families covering management, operational, and technical controls;
- A separate privacy control catalog (Appendix J) covering the Fair Information Practice Principles;
- Three baseline security control sets (low-impact, moderate-impact, and high-impact) based on FIPS 199 security categorization;
- A control tailoring process that allows organizations to adjust baselines for their specific mission, threat environment, and operating conditions;
- Overlay templates that enable communities of interest to create specialized control baselines (e.g., healthcare, industrial control systems);
- Assurance and trustworthiness guidance for selecting and implementing controls that meet specified levels of assurance.

NIST SP 800-53 r4 is the foundational control catalog referenced by federal regulations (including the HIPAA Security Rule via NIST SP 800-66), industry frameworks (HITRUST CSF, FedRAMP, CMMC), and many state and private-sector security programs. For healthcare organizations, SP 800-53 controls map directly to HIPAA Security Rule standards through the SP 800-66 Appendix D crosswalk.

Document Organization

NIST SP 800-53 r4 is organized into three chapters and ten appendices:

Chapter 1 — Introduction	Purpose, target audience, applicability, organization of the publication, and relationships to other NIST publications.
Chapter 2 — The Fundamentals	Multitiered organization-wide risk management, security control structure, control baselines, common controls, security control designations, external service providers, assurance and trustworthiness, and revisions and extensions.
Chapter 3 — The Process	Selecting security control baselines, tailoring baseline security controls (applying scoping considerations, selecting compensating security controls, assigning security control parameter values, supplementing baseline security controls, providing additional specification information for implementation), creating overlays, documenting the security control selection process, and applying the methodology in new and legacy systems.
Appendix A — References	Laws, policies, directives, instructions, standards, and guidelines applicable to security control selection and use.
Appendix B — Glossary	Common terms and definitions used in the publication.

Appendix C — Acronyms	Common abbreviations used in the publication.
Appendix D — Security Control Baselines (Summary)	Low-impact, moderate-impact, and high-impact baseline allocations for every security control in the catalog.
Appendix E — Assurance and Trustworthiness	Properties of assurance, developmental and operational assurance, and the relationship between trustworthiness and assurance.
Appendix F — Security Control Catalog	Comprehensive catalog of security controls in 18 control families. This is the bulk of the document.
Appendix G — Information Security Programs	Program management (PM) family controls for organization-wide information security programs.
Appendix H — International Information Security Standards	Mappings between NIST SP 800-53 controls and ISO/IEC 27001:2013 controls.
Appendix I — Overlay Template	Standardized template for developing community-specific or specialized security control overlays.
Appendix J — Privacy Control Catalog	Comprehensive catalog of privacy controls in 8 privacy control families (Authority and Purpose, Accountability/Audit/Risk Management, Data Quality and Integrity, Data Minimization and Retention, Individual Participation and Redress, Security, Transparency, Use Limitation).

The 18 Security Control Families

NIST SP 800-53 r4 organizes security controls into 18 families. Each family is identified by a two-letter abbreviation that prefixes the individual control numbers within that family (e.g., AC-1, AC-2, AC-3 are the first three controls in the Access Control family).

NIST SP 800-53 r4 — Security Control Families		
ID	Family	Focus
AC	Access Control	Account management, access enforcement, separation of duties, least privilege, unsuccessful logon attempts, system use notification, session lock, remote access, wireless access, mobile devices, use of external information systems.

ID	Family	Focus
AT	Awareness and Training	Security awareness training, role-based security training, security training records.
AU	Audit and Accountability	Audit events, content of audit records, audit storage capacity, response to audit processing failures, audit review/analysis/reporting, audit reduction and report generation, time stamps, protection of audit information, non-repudiation, audit record retention.
CA	Security Assessment and Authorization	Security assessments, system interconnections, plan of action and milestones, security authorization, continuous monitoring, penetration testing, internal system connections.
CM	Configuration Management	Baseline configuration, configuration change control, security impact analysis, access restrictions for change, configuration settings, least functionality, information system component inventory, configuration management plan, software usage restrictions, user-installed software.
CP	Contingency Planning	Contingency plan, contingency training, contingency plan testing, alternate storage site, alternate processing site, telecommunications services, information system backup, information system recovery and reconstitution, alternate communications protocols.
IA	Identification and Authentication	Identification and authentication (organizational users and non-organizational users), device identification and authentication, identifier management, authenticator management, authenticator feedback, cryptographic module authentication, re-authentication.
IR	Incident Response	Incident response training, incident response testing, incident handling, incident monitoring, incident reporting, incident response assistance, incident response plan, information spillage response.
MA	Maintenance	System maintenance policy and procedures, controlled maintenance, maintenance tools, nonlocal maintenance, maintenance personnel, timely maintenance.
MP	Media Protection	Media access, media marking, media storage, media transport, media sanitization, media use, media downgrading.
PE	Physical and Environmental Protection	Physical access authorizations, physical access control, access control for transmission medium, access control for output devices, monitoring physical access, visitor access records, power equipment and cabling, emergency shutoff, emergency power, emergency lighting, fire protection, temperature and humidity controls, water damage protection, delivery and removal, alternate work site, location of information system components.
PL	Planning	Security planning policy and procedures, system security plan, rules of behavior, information security architecture, central management.
PM	Program Management	Information security program plan, senior information security officer, information security resources, plan of action and milestones process, information system inventory, information security measures of performance, enterprise architecture,

ID	Family	Focus
		critical infrastructure plan, risk management strategy, security authorization process, mission/business process definition, insider threat program, information security workforce, testing/training/monitoring, contacts with security groups and associations, threat awareness program.
PS	Personnel Security	Position risk designation, personnel screening, personnel termination, personnel transfer, access agreements, third-party personnel security, personnel sanctions.
RA	Risk Assessment	Risk assessment policy and procedures, security categorization, risk assessment, vulnerability scanning, technical surveillance countermeasures survey.
SA	System and Services Acquisition	Allocation of resources, system development life cycle, acquisition process, information system documentation, security engineering principles, external information system services, developer configuration management, developer security testing and evaluation, supply chain protection, trustworthiness, criticality analysis, development process/standards/tools, developer-provided training, developer security architecture and design, tamper resistance and detection, component authenticity, customized development of critical components.
SC	System and Communications Protection	Application partitioning, security function isolation, information in shared resources, denial of service protection, resource availability, boundary protection, transmission confidentiality and integrity, network disconnect, cryptographic key establishment and management, cryptographic protection, collaborative computing devices, transmission of security attributes, public key infrastructure certificates, mobile code, voice over Internet Protocol, secure name/address resolution service, session authenticity, fail in known state, thin nodes, honeypots, platform-independent applications, protection of information at rest, heterogeneity, concealment and misdirection, covert channel analysis, information system partitioning, transmission preparation integrity, non-modifiable executable programs, honey clients, distributed processing and storage, out-of-band channels, operations security, process isolation, wireless link protection, port and I/O device access, sensor capability and data, usage restrictions, detonation chambers.
SI	System and Information Integrity	Flaw remediation, malicious code protection, information system monitoring, security alerts and advisories, security function verification, software/firmware/information integrity, spam protection, information input validation, error handling, information handling and retention, predictable failure prevention, non-persistence, information output filtering, memory protection, fail-safe procedures.

Security Control Structure

Each control in the SP 800-53 r4 catalog follows a consistent structure:

- **Control section** — Concise statement of the specific security capability needed to protect the information system.
- **Supplemental Guidance section** — Non-prescriptive additional information that provides important considerations for implementing the control.

- **Control Enhancements section** — Statements of security capability to (i) add functionality/specificity to a base control; and/or (ii) increase the strength of a base control. Control enhancements are numbered sequentially within each control (e.g., AC-2(1), AC-2(2)).
- **References section** — Specific publications (e.g., FIPS, NIST SP, federal directives) related to the control.
- **Priority and Baseline Allocation section** — Recommended priority code (P1, P2, P3 or P0) for control implementation and the allocation of the control across the three baselines (Low, Moderate, High).

For example, control **AC-2 Account Management** has a base control statement, supplemental guidance covering ~20 considerations, 13 control enhancements (AC-2(1) through AC-2(13)), references to related publications, and baseline allocations indicating it is required in all three baselines with specific enhancements required at moderate and high.

Security Control Baselines

Appendix D of SP 800-53 r4 provides three baseline security control sets corresponding to the FIPS 199 impact levels:

Low-Impact Baseline

Applies to information systems where the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. The low baseline includes a foundational subset of controls and few control enhancements.

Moderate-Impact Baseline

Applies to information systems where the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect. The moderate baseline adds controls and enhancements beyond the low baseline. This is the most commonly applicable baseline for typical healthcare/EPHI systems.

High-Impact Baseline

Applies to information systems where the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect. The high baseline adds further controls and enhancements beyond the moderate baseline.

Tailoring the Baseline

Organizations are expected to tailor the selected baseline for their specific operating environment using a documented tailoring process. Tailoring activities include:

- **Identifying and designating common controls** in initial security control baselines.
- **Applying scoping considerations** to the remaining baseline security controls (e.g., technology-related considerations, mission/business-related considerations, operational/environmental-related considerations).
- **Selecting compensating security controls**, if needed, when a baseline control cannot be implemented as written.
- **Assigning specific values to organization-defined security control parameters** via explicit assignment and selection statements (e.g., the parameter [Assignment: organization-defined frequency] gets a specific value like "annually").

- **Supplementing baselines with additional security controls and control enhancements**, if needed, based on organizational risk assessments.
- **Providing additional specification information** for control implementation, if needed.

Overlays

An overlay is a specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, intended to complement the more generic security control baselines. Overlays facilitate consistent and repeatable security control selection within specific communities or use cases. Examples include healthcare overlays for HIPAA-regulated environments, industrial control systems overlays, cloud computing overlays, and national security system overlays. Appendix I of SP 800-53 r4 provides a standardized overlay template.

Privacy Control Catalog (Appendix J)

Beyond the security control catalog, Rev 4 introduced a separate privacy control catalog (Appendix J) covering eight privacy control families based on the Fair Information Practice Principles (FIPPs):

AP — Authority and Purpose

Authority to collect, purpose specification.

AR — Accountability, Audit, and Risk Management

Governance and privacy program; privacy impact and risk assessment; privacy requirements for contractors and service providers; privacy monitoring and auditing; privacy awareness and training; privacy reporting; privacy-enhanced system design and development; accounting of disclosures.

DI — Data Quality and Integrity

Data quality, data integrity and data integrity board.

DM — Data Minimization and Retention

Minimization of personally identifiable information; data retention and disposal; minimization of PII used in testing/training/research.

IP — Individual Participation and Redress

Consent; individual access; redress; complaint management.

SE — Security

Inventory of personally identifiable information; privacy incident response.

TR — Transparency

Privacy notice; system of records notices and privacy act statements; dissemination of privacy program information.

UL — Use Limitation

Internal use; information sharing with third parties.

Connecting SP 800-53 to the HIPAA Security Rule

The HIPAA Security Rule and NIST SP 800-53 r4 are complementary frameworks. SP 800-53 r4 provides the detailed control catalog; the HIPAA Security Rule provides the regulatory requirements specific to electronic protected health information (EPHI). NIST SP 800-66 Rev 1, Appendix D (covered in CSR HIPAA Library — Premium Edition Paper 09) provides a comprehensive crosswalk between every HIPAA standard and the relevant SP 800-53 control families.

Common SP 800-53 control families that map directly to HIPAA requirements include:

- **RA** (Risk Assessment) → HIPAA § 164.308(a)(1)(ii)(A) Risk Analysis
- **AC** (Access Control) → HIPAA § 164.308(a)(4), § 164.312(a)(1)
- **AT** (Awareness and Training) → HIPAA § 164.308(a)(5) Security Awareness and Training
- **AU** (Audit and Accountability) → HIPAA § 164.312(b) Audit Controls
- **CP** (Contingency Planning) → HIPAA § 164.308(a)(7) Contingency Plan
- **IA** (Identification and Authentication) → HIPAA § 164.312(d) Person or Entity Authentication
- **IR** (Incident Response) → HIPAA § 164.308(a)(6) Security Incident Procedures
- **MP** (Media Protection) → HIPAA § 164.310(d) Device and Media Controls
- **PE** (Physical and Environmental Protection) → HIPAA § 164.310(a) Facility Access Controls
- **PS** (Personnel Security) → HIPAA § 164.308(a)(3) Workforce Security
- **SC** (System and Communications Protection) → HIPAA § 164.312(e)(1) Transmission Security
- **SI** (System and Information Integrity) → HIPAA § 164.312(c)(1) Integrity
- **PM** (Program Management) → HIPAA § 164.308(a)(2) Assigned Security Responsibility; § 164.316 Policies and Procedures and Documentation

How to Use This Edition Alongside the Original PDF

This CSR-branded Executive Summary is best used in tandem with the full NIST SP 800-53 r4 PDF:

1. Start here to understand the document's structure, the 18 control families, baseline selection, and the tailoring process.
2. Use the original NIST PDF (Appendix F) when you need the exact wording of an individual control, its supplemental guidance, its enhancements, and its references.
3. Use Appendix D of the original NIST PDF to look up baseline allocations for a specific control.
4. Use the SP 800-66 Rev 1 Appendix D crosswalk (covered in CSR HIPAA Library — Premium Edition Paper 09) to map HIPAA Security Rule standards to SP 800-53 control families when building your security program.

Appendix C — Acronyms

CFR	Code of Federal Regulations
CNSS	Committee on National Security Systems
CNSSI	Committee on National Security Systems Instruction
CSRC	Computer Security Resource Center
DoD	Department of Defense
EO	Executive Order
FBI	Federal Bureau of Investigation
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
IR	Interagency Report
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency

OMB	Office of Management and Budget
------------	---------------------------------

PII	Personally Identifiable Information
------------	-------------------------------------

PIV	Personal Identity Verification
------------	--------------------------------

RMF	Risk Management Framework
------------	---------------------------

SP	Special Publication
-----------	---------------------

USC	United States Code
------------	--------------------

SOURCE OF TRUTH

For the full 462-page NIST SP 800-53 r4 — including every control statement, supplemental guidance paragraph, control enhancement, reference, and baseline allocation — see the original NIST publication: *"NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations,"* April 2013 (updates as of 01-22-2015), available at <http://dx.doi.org/10.6028/NIST.SP.800-53r4> and from your CSR HIPAA Library archive.



CYBER SECURITY RESOURCE
PROTECTING DATA · SECURING TRUST

About Cyber Security Resource

Protecting Data — Securing Trust

We're a healthcare-focused cybersecurity firm. We help medical technology, SaaS, and regulated organizations build security programs that hold up — under audit, under attack, and under board scrutiny.

Our approach is structured and cost-effective. We focus on practical risk management, compliance alignment, and real-world security testing. The goal is simple: **meet HIPAA, HITRUST, and enterprise customer requirements with confidence** — without spending a year and six figures to get there.

This library is the same orientation we hand a new client on day one. Use it as a working reference; the requirements are unchanged from the original CMS guidance, and the design is built to be readable in a boardroom or on a security analyst's second monitor.

CONTACT

support@cybersecurityresource.com
+1 (442) 222-1338

HEADQUARTERS

Carlsbad, California
United States

WEB · EDITION

cybersecurityresource.com
Cyber Security Resource Edition ·
2026