GOVDATAHOSTING
POWERED BY IT-CNP, INC.

FEDRAMP HIGH (CLASS D) CERTIFIED CLOUD PLATFORM

NIST 800-53 REV 5
CONTROL MATRIX COMPANION GUIDE

Your Practical Guide to Federal Security Compliance

2026 EDITION • **HIGH BASELINE · FISMA · FEDRAMP**

INSIDE THIS GUIDE

Introduction to NIST 800-53 Rev 5 • How to use the control matrix • Control family quick reference • Control inheritance explained • Implementation roadmap • Next steps with GovDataHosting

FOR

Compliance Teams • ISSOs & ISSMs • Federal Contractors

GovDataHosting

FedRAMP High (Class D) Certified • NIST 800-53 Rev 5 High • DoD IL2 Authorized

www.govdatahosting.com | 800-967-1004

What's Inside

01 Introduction to NIST 800-53 Rev 5
What changed from Revision 4, the 20 control families, and how baselines map to FedRAMP

02 How to Use the Control Matrix
Navigating the workbook, filtering by your requirements, and mapping to your SSP

03 Control Family Quick Reference
Purpose, key controls, challenges, and inheritance for each High-baseline family

04 The Control Inheritance Advantage
Shared responsibility, how certification enables inheritance, and documentation

05 Implementation Roadmap
A phased, prioritized path from foundational controls to continuous monitoring

06 Next Steps with GovDataHosting
Free consultation, readiness assessment, and additional resources

Introduction to NIST 800-53 Rev 5

NIST Special Publication 800-53 Revision 5 represents the most comprehensive update to federal security controls in over a decade. It reflects the evolving threat landscape, incorporates lessons learned from major security incidents, and provides a more flexible, outcome-focused approach to security and privacy.

What Changed from Revision 4

- **New control families:** two families were added — PT (PII Processing and Transparency) for privacy, and SR (Supply Chain Risk Management) for supply chain security.
- **Privacy integration:** privacy controls are now integrated throughout the catalog rather than maintained as a separate overlay.
- **Outcome-based focus:** controls emphasize security outcomes rather than prescriptive implementation methods, giving organizations more flexibility.
- **State-of-practice updates:** controls reflect current best practices, including cloud security, mobile device management, and continuous monitoring.
- **Control reorganization:** some controls have been consolidated, split, or moved between families for clearer logical grouping.

The 20 Control Families

NIST 800-53 Rev 5 organizes security and privacy controls into 20 families, each addressing a specific aspect of information security. The accompanying Excel workbook provides detailed control information for each family.

CODE	FAMILY NAME	PRIMARY FOCUS
AC	**Access Control**	Limit system access to authorized users and protect against unauthorized access
AT	**Awareness and Training**	Ensure personnel are adequately trained on security responsibilities
AU	**Audit and Accountability**	Create, protect, and retain system audit records
CA	**Assessment, Authorization, and Monitoring**	Assess security controls and authorize system operation
CM	**Configuration Management**	Establish and maintain baseline configurations
CP	**Contingency Planning**	Ensure system availability and recovery capability
IA	**Identification and Authentication**	Identify and authenticate users and devices
IR	**Incident Response**	Detect, respond to, and recover from security incidents
MA	**Maintenance**	Perform timely system maintenance
MP	**Media Protection**	Protect system media containing sensitive information

CODE	FAMILY NAME	PRIMARY FOCUS
PE	**Physical and Environmental Protection**	Limit physical access and protect against environmental hazards
PL	**Planning**	Develop security plans and rules of behavior
PM	**Program Management**	Organization-wide security and privacy program controls (not allocated to baselines)
PS	**Personnel Security**	Ensure personnel trustworthiness and manage access appropriately
PT	**PII Processing and Transparency**	Privacy controls governing the processing of personally identifiable information
RA	**Risk Assessment**	Identify and assess security risks
SA	**System and Services Acquisition**	Incorporate security into the system development lifecycle
SC	**System and Communications Protection**	Monitor and protect communications and system boundaries
SI	**System and Information Integrity**	Protect systems and information from compromise
SR	**Supply Chain Risk Management**	Manage supply chain security risks

Understanding Control Baselines

Control baselines are pre-defined sets of security controls selected by system impact level. Impact level is determined through FIPS 199 categorization based on potential impact to confidentiality, integrity, and availability. The counts below match the accompanying workbook.

- **Low baseline (~156 controls):** for systems where loss of confidentiality, integrity, or availability would have a limited adverse effect.
- **Moderate baseline (~325 controls):** for systems where loss would have a serious adverse effect. This is the most common baseline for federal systems.
- **High baseline (434 controls):** for systems where loss would have a severe or catastrophic adverse effect — national security systems, high-value assets, and the most sensitive unclassified data. This is the baseline detailed in this guide and the accompanying workbook.

Note: these totals reflect the NIST 800-53 baselines as tallied in the accompanying workbook. FedRAMP applies additional tailoring to these baselines — the FedRAMP High baseline totals approximately 410 controls — so a FedRAMP authorization package may show slightly different counts than this NIST-based matrix.

High vs. Moderate Baseline

The High baseline builds on Moderate with roughly 109 additional controls and enhancements, plus stricter parameters on shared controls. The difference is as much about depth and rigor as raw count.

CATEGORY	MODERATE BASELINE	HIGH BASELINE
Total controls	~325	**434 (+109)**
Control enhancements	Basic enhancements	Advanced, more robust implementations
Typical systems	Most federal systems	National security systems and high-value assets
Assessment rigor	Annual + continuous monitoring	Annual + enhanced continuous monitoring

Key additional requirements introduced at the High baseline include:

- **Enhanced monitoring —** more extensive system monitoring and real-time alerting
- **Stronger authentication —** additional MFA requirements and session controls
- **Advanced incident response —** insider-threat handling and information-spillage procedures
- **Rigorous change control —** cryptographic key management and automated verification
- **Supply chain security —** tamper resistance and enhanced component authenticity
- **Network isolation —** security-function isolation and fail-secure requirements

> **NOTE: BASELINE TERMINOLOGY IS CHANGING**
> Under FedRAMP's Consolidated Rules for 2026 (CR26), the Low, Moderate, and High baselines are being relabeled as Certification Classes B, C, and D respectively (with a new Class A pilot tier). The underlying control sets remain largely the same, and existing authorizations carry over. GovDataHosting is **FedRAMP High (Class D) Certified**.

How Controls Map to FedRAMP

FedRAMP (the Federal Risk and Authorization Management Program) uses NIST 800-53 as its security control framework. FedRAMP baselines align closely with the NIST baselines but add FedRAMP-specific parameters and requirements. When you deploy on a **FedRAMP-certified** infrastructure provider like GovDataHosting, you can inherit a significant portion of your required controls — dramatically reducing your compliance burden.

How to Use This Control Matrix

The accompanying Excel workbook is designed to be a practical, working tool for your compliance team. This section explains how to get the most value from the matrix.

Navigating the Workbook

- **Overview Dashboard:** a high-level summary of control counts, inheritance statistics, and family breakdowns. Start here to understand the scope of your compliance effort.
- **Master Control Matrix:** a complete listing of all High-baseline controls with Moderate/High applicability, inheritance status, priority, assessment frequency, and evidence types. Use filters to focus on specific areas.
- **Inheritance Summary:** a grouped view of controls by inheritance type (Fully Inherited, Partially Inherited, Customer Implements). Essential for SSP documentation.
- **High vs. Moderate:** a side-by-side comparison of the two baselines, including the additional controls and rigor introduced at High.
- **Rev 5 Changes:** a reference for organizations transitioning from Revision 4 to Revision 5.

Filtering by Your Requirements

- **By baseline:** filter the Moderate or High columns to see which controls apply to your system's impact level.
- **By inheritance:** filter the GovDataHosting Inheritance column to identify controls you must implement versus those you can inherit.
- **By priority:** filter by implementation priority to focus on Critical and High-priority controls first.
- **By family:** filter by family to work through controls systematically during implementation or assessment.

Mapping to Your SSP

Your System Security Plan (SSP) must document how each applicable control is implemented. The matrix supports this by providing:

- **Control descriptions** so you understand what each control requires
- **Inheritance status** to identify which controls reference GovDataHosting's implementation
- **Evidence types** to guide your documentation and artifact collection
- **Assessment frequency** to plan your continuous monitoring activities

Control Family Quick Reference

This quick reference summarizes 18 control families — the operational and technical families most relevant to a High-baseline implementation — with each family's purpose, key controls, common challenges, and the share of controls that can be fully or partially inherited from GovDataHosting.

Two families are not given individual rows: **Program Management (PM)** applies organization-wide and is not allocated to impact baselines, and **PII Processing and Transparency (PT)** privacy controls are detailed in the accompanying workbook.

CONTROL FAMILY	KEY CONTROLS	COMMON CHALLENGES	INHERIT
AC Access Control *Limit access to authorized users*	AC-2 (Account Management), AC-3 (Access Enforcement), AC-6 (Least Privilege), AC-17 (Remote Access)	Managing accounts across hybrid environments, enforcing least privilege, securing remote access	83%
AT Awareness and Training *Train personnel on security*	AT-2 (Literacy Training), AT-3 (Role-Based Training)	Keeping training current, documenting completion, role-specific requirements	56%
AU Audit and Accountability *Create, protect, retain audit records*	AU-2 (Event Logging), AU-6 (Audit Review), AU-9 (Protection of Audit Information)	Log aggregation across systems, storage capacity, timely review and analysis	93%
CA Assessment, Authorization, and Monitoring *Assess controls and authorize operation*	CA-2 (Control Assessments), CA-5 (POA&M), CA-7 (Continuous Monitoring)	Assessment objectivity, POA&M management, continuous-monitoring implementation	33%
CM Configuration Management *Maintain baseline configurations*	CM-2 (Baseline Configuration), CM-6 (Configuration Settings), CM-8 (Component Inventory)	Drift detection, change control across environments, accurate inventory	97%
CP Contingency Planning *Ensure availability and recovery*	CP-2 (Contingency Plan), CP-9 (System Backup), CP-10 (Recovery and Reconstitution)	Testing backup/recovery, alternate sites, meeting RTO/RPO targets	97%
IA Identification and Authentication *Authenticate users and devices*	IA-2 (Organizational Users), IA-5 (Authenticator Management), IA-8 (Non-Organizational Users)	MFA implementation, credential management, PIV integration	94%
IR Incident Response *Detect, respond, recover*	IR-4 (Incident Handling), IR-6 (Incident Reporting), IR-8 (Incident Response Plan)	Timely detection, coordinated response, evidence preservation, reporting	88%
MA Maintenance *Perform timely maintenance*	MA-2 (Controlled Maintenance), MA-4 (Nonlocal Maintenance), MA-5 (Maintenance Personnel)	Scheduling maintenance windows, controlling remote-maintenance access	75%
MP Media Protection *Protect sensitive media*	MP-4 (Media Storage), MP-5 (Media Transport), MP-6 (Media Sanitization)	Tracking media, ensuring sanitization, controlling portable storage	83%

CONTROL FAMILY	KEY CONTROLS	COMMON CHALLENGES	INHERIT
PE Physical and Environmental Protection *Limit physical access*	PE-2 (Physical Access Authorizations), PE-3 (Physical Access Control), PE-6 (Monitoring)	Visitor management, environmental monitoring, emergency procedures	**76%**
PL Planning *Develop security plans*	PL-2 (System Security Plan), PL-4 (Rules of Behavior), PL-8 (Security Architecture)	Keeping the SSP current, enforcing rules of behavior, architecture documentation	**50%**
PS Personnel Security *Ensure personnel trustworthiness*	PS-3 (Personnel Screening), PS-4 (Personnel Termination), PS-6 (Access Agreements)	Background-check requirements, timely access revocation, contractor management	**25%**
RA Risk Assessment *Identify and assess risk*	RA-3 (Risk Assessment), RA-5 (Vulnerability Scanning), RA-7 (Risk Response)	Current threat information, vulnerability prioritization, risk-acceptance decisions	**53%**
SA System and Services Acquisition *Build security into the SDLC*	SA-4 (Acquisition Process), SA-9 (External System Services), SA-11 (Developer Testing)	Supply chain security, developer requirements, external-service agreements	**33%**
SC System and Communications Protection *Protect comms and boundaries*	SC-7 (Boundary Protection), SC-8 (Transmission Protection), SC-28 (Protection at Rest)	Boundary definition, encryption implementation, network segmentation	**76%**
SI System and Information Integrity *Protect against compromise*	SI-2 (Flaw Remediation), SI-3 (Malicious Code Protection), SI-4 (System Monitoring)	Patch management, malware protection, intrusion detection	**88%**
SR Supply Chain Risk Management *Manage supply chain risk*	SR-2 (SCRM Plan), SR-3 (Supply Chain Controls), SR-6 (Supplier Assessments)	Supplier visibility, component authenticity, notification agreements	**93%**

READING THE INHERITANCE COLUMN

Inheritance percentages reflect the share of a family's High-baseline controls GovDataHosting can fully or partially satisfy on your behalf. High-inheritance families (e.g., CM, CP, IA, AU) are infrastructure- and platform-centric; lower-inheritance families (e.g., PS, CA, SA) are policy- and personnel-centric and remain primarily your responsibility. Confirm current figures against the accompanying workbook.

The Control Inheritance Advantage

Control inheritance is one of the most powerful tools available to reduce your compliance burden. When you deploy your system on GovDataHosting's FedRAMP High (Class D) Certified infrastructure, you can inherit a significant portion of the required security controls.

Understanding Shared Responsibility

In cloud environments, security responsibility is shared between the Cloud Service Provider (CSP) and the customer. The division depends on the service model:

- **Infrastructure as a Service (IaaS):** the CSP manages physical security, virtualization, and network infrastructure; the customer manages operating systems, applications, and data.
- **Platform as a Service (PaaS):** the CSP additionally manages operating systems and runtime environments; the customer manages applications and data.
- **GovDataHosting's bundled approach:** our FedRAMP High (Class D) Certified platform bundles infrastructure, security controls, monitoring, and compliance support — maximizing what you can inherit.

How FedRAMP Certification Enables Inheritance

GovDataHosting has undergone rigorous third-party assessment and achieved FedRAMP High (Class D) Certification. This means:

- **Controls are assessed:** an independent 3PAO has verified that GovDataHosting implements all required High-baseline controls.
- **Documentation exists:** detailed control-implementation statements are available for you to reference in your SSP.
- **Continuous monitoring:** GovDataHosting maintains ongoing monitoring, scanning, and reporting that supports your authorization, operated by our 24/7 U.S.-based SOC.
- **Customer responsibility matrix:** clear documentation of which controls you inherit and what customer responsibilities remain.

Documentation Requirements for Inherited Controls

Even for inherited controls, your SSP must document the inheritance relationship. For each inherited control, you should:

- Identify the control as inherited from GovDataHosting
- Reference GovDataHosting's FedRAMP certification package
- Document any customer-specific configurations or responsibilities
- Explain how the inherited control applies to your specific system

GOVDATAHOSTING INHERITANCE IMPACT

On GovDataHosting's FedRAMP High (Class D) Certified infrastructure, High-baseline customers typically:

- **Inherit ~38% of controls fully** (165 of 434 — GovDataHosting implements completely)
- **Share responsibility for ~39% of controls** (169 of 434 — reduced documentation burden)
- **Implement ~23% independently** (100 of 434 — policies, procedures, personnel)

Result: you can fully or partially inherit ~77% of the High baseline (334 of 434 controls), for an estimated 1,900+ hours saved on your path to ATO. (Inheritance figures are GovDataHosting estimates from the accompanying workbook; confirm against your current package.)

Implementation Roadmap

Successfully implementing NIST 800-53 controls requires a structured, phased approach. This roadmap provides a framework for prioritizing and implementing controls effectively.

Phase 1 — Critical Controls (Days 1–60)

Focus first on foundational controls that enable other security measures:

- **Policy framework (all "-1" controls):** develop security policies and procedures for each control family to establish your organizational posture.
- **Access control foundation (AC-2, AC-3, AC-6):** establish account management, access enforcement, and least privilege.
- **Audit and logging (AU-2, AU-3, AU-6):** implement event logging and review — without audit trails you cannot detect or investigate incidents.
- **System Security Plan (PL-2):** begin documenting your security implementation; the SSP is your primary authorization artifact.

Phase 2 — High-Priority Controls (Days 60–120)

Build on the foundation with controls that address common threats:

- **Configuration management (CM-2, CM-6, CM-7):** establish baseline configurations, configuration settings, and least functionality.
- **Identification and authentication (IA-2, IA-5):** implement strong authentication, including MFA for all users.
- **System protection (SC-7, SC-8, SC-28):** configure boundary protection, transmission security, and encryption at rest.
- **Vulnerability management (RA-5, SI-2):** implement vulnerability scanning and flaw-remediation processes.

Phase 3 — Remaining Controls (Days 120+)

Complete implementation of remaining controls and prepare for assessment:

- **Incident response (IR-4, IR-6, IR-8):** finalize incident-handling procedures and reporting mechanisms.
- **Contingency planning (CP-2, CP-9, CP-10):** complete contingency plans and test backup/recovery procedures.
- **Supply chain (SR-2, SR-3):** implement supply chain risk-management controls.
- **Assessment preparation:** compile evidence artifacts, complete SSP documentation, and conduct an internal assessment.

Continuous Monitoring Requirements

Authorization is not a one-time event. Continuous monitoring is required to maintain your ATO:

- **Vulnerability scanning:** monthly for all systems, with immediate scanning after significant changes.

- **POA&M management:** monthly review and update of the Plan of Action and Milestones.
- **Control assessment:** annual assessment of all controls, with a subset assessed monthly.
- **SSP updates:** annual review and update, or after significant system changes.

Next Steps with GovDataHosting

Ready to accelerate your compliance journey? GovDataHosting provides everything you need to achieve and maintain federal authorization efficiently.

Free Compliance Consultation

Schedule a complimentary 30-minute consultation with our compliance experts to assess your current state and develop a customized roadmap to authorization.

FREE ATO READINESS ASSESSMENT

Schedule a complimentary 30-minute consultation with our compliance experts to assess your current state and build a customized roadmap to authorization.

800-967-1004

www.govdatahosting.com/contact-us • **info@govdatahosting.com**

Additional Resources

- **Complete FISMA Authorization Guide —** a step-by-step guide to achieving FISMA authorization
- **FedRAMP Certification Playbook —** methodology for achieving FedRAMP certification
- **SSP Template Library —** editable templates aligned to NIST requirements
- **Total Cost of Ownership Calculator —** compare bundled vs. multi-vendor approaches

A Division of IT-CNP, Inc. • Founded 2001

FedRAMP High (Class D) Certified • DoD IL2 Authorized • NIST 800-53 Rev 5 High • SOC 2 Type II • ISO 27001

DISCLAIMER

The information in this guide is accurate as of the date of publication. The NIST 800-53 control catalog (updated to Rev 5.2.0 in 2025), FedRAMP baselines and policy (including the CR26 / FedRAMP 20x transition and the Low/Moderate/High to Class B/C/D relabeling), and control counts and inheritance figures evolve over time and are subject to change. This guidance can change rapidly. Always verify the latest requirements at authoritative sources such as csrc.nist.gov and fedramp.gov before making compliance decisions.