

GOVERNANCE DOCS

NIST RMF (SP 800-37 Rev. 2)

Gap Assessment Report

NIST Risk Management Framework for Information Systems and Organizations

Capitol Benefits Systems (sample)

The benefits case management system and its hosting environment, categorised as moderate impact.

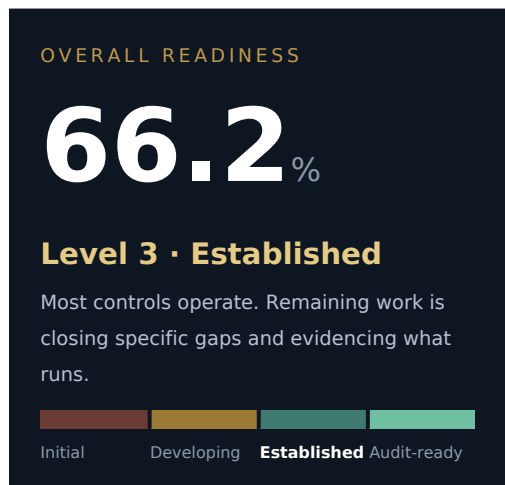
ASSESSED	25 September 2026
EDITION	Special Publication 800-37 Revision 2, December 2018
IN SCOPE	53 requirements, 51 applicable
PROFILE	Government and public sector · 50 to 249 people
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Capitol Benefits Systems (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Capitol Benefits Systems (sample) stands against NIST RMF



APPLICABLE	EVIDENCED	OPEN GAPS	HIGH PRIORITY
51	18	33	12

STATUS OF EVERY REQUIREMENT



GAPS WITH AN OWNER	WITH A TARGET DATE	NOT ANSWERED
15 of 33	9 of 33	0

WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 66.2% against NIST RMF across 51 applicable controls. 18 of them are implemented and evidenced.
- Most open gaps: Authorize, with 6 at 42%. Strongest area: Categorize at 88%.
- 11 controls are operating but not evidenced. Collecting their records alone lifts the score to 71.6% (+5.4 points), the cheapest gain available.
- 12 gaps are high priority (not started or only planned); 3 of them are in Authorize.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 3 high-priority gaps in Authorize	Compliance Lead	Risk Assessment Report
2	MEDIUM	Adopt and tailor the Management Support Letter, which closes 3 open gaps	To assign	Management Support Letter
3	LOW	Evidence the 11 controls that already operate (+5.4 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

The organization achieved a 66% score at Established readiness; closing 12 high priority gaps is the next essential move.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

The organization has attained Established readiness with an overall score of 66.2%, confirming that primary operational controls function across most departments. However, 12 high priority gaps in system authorization, risk determination, and implementation tracking introduce governance risk. Leadership must formally approve risk tolerance baselines, assign owners to the remaining 18 unassigned gaps, and authorize resource allocation to complete 10 planned controls across the next 90 days.

WHERE YOU STAND

The organization reached an overall score of 66.2% across 51 applicable requirements, placing readiness at level 3 of 4, named Established. Most controls operate across the enterprise, but 33 open gaps remain. Among these gaps, 12 are rated high priority. Currently, 18 requirements are implemented and evidenced, while 11 are implemented without evidence. Formal ownership is assigned to 15 gaps, and 9 gaps have target completion dates.

WHAT IT MEANS FOR THE ORGANIZATION

The pattern indicates mature operational capabilities in areas such as Categorize at 87.5% and Assess at 85.7%, yet foundational governance lags behind. Significant exposure exists in Implement at 25% and Authorize at 41.7%. Without formal risk determinations and signed authorizations, operational controls lack documented leadership oversight. Furthermore, leaving 11 implemented controls unevidenced creates unnecessary gaps in accountability during review, despite day-to-day practices already running.

WHERE TO FOCUS FIRST

Initial attention must center on the 2 unstarted high priority items in Implement and Authorize. Documenting risk determinations and updating control implementation data immediately strengthens operational oversight. Next, the organization should formalize planned activities in Prepare and Monitor, such as defining risk management strategies and ongoing response procedures. Securing documented evidence for controls that are already working will quickly raise the assessment score to 71.6%.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Establish implementation records and change controls I-2 Update control implementation information · I-2b Change control during build	Failing to record control implementation data and build changes leaves system configurations unverified. This undermines system stability and weakens traceability across operational baselines.	Draft configuration update tracking using the Change Management Policy.	Change Management Policy NIST Cyber Risk Management Toolkit	30 DAYS
2 Complete risk determination and formal authorization decisions R-2 Risk analysis and determination · R-4 Authorisation decision	Operating systems without formal risk analysis and authorization decisions exposes the organization to unapproved operational liabilities. Explicit management sign-off confirms risk acceptance.	Compile the Risk Assessment Report to determine outstanding system risks.	Risk Assessment Report NIST Cyber Risk Management Toolkit	30 DAYS
3 Formalize organization risk strategy and impact prioritization P-2 Risk management strategy · P-6 Impact-level prioritisation	Without a consolidated organizational risk strategy, security investments cannot be aligned to mission priorities. This creates inconsistent protection levels across systems.	Review the Cyber Security Risk Management Framework with designated system owners.	Cyber Security Risk Management Framework NIST Cyber Risk Management Toolkit	60 DAYS
4 Operationalize ongoing risk response and authorization updates M-3 Ongoing risk response · M-4 Authorisation package updates	Static authorizations fail to capture active threats and operational changes. Maintaining ongoing response plans ensures risks are addressed continuously.	Establish review cycles using the Vulnerability Management Policy.	Vulnerability Management Policy NIST Cyber Risk Management Toolkit	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS

- Review the Change Management Policy to record all control implementation data.
- Generate the Risk Assessment Report for pending system authorization packages.
- Collect existing documentation to validate 11 implemented but unevidenced controls.
- Assign designated owners and target completion dates to all 33 open gaps.

DAYS 31 TO 60

- Adopt the Cyber Security Risk Management Framework across all operational units.
- Publish the Data Retention Policy and complete information life cycle planning.
- Implement the Configuration Management Procedure to formalize control build tracking.
- Issue the Management Support Letter for plan review and approval.

DAYS 61 TO 90

- Execute ongoing risk response measures using the Vulnerability Management Policy.
- Schedule periodic reviews to maintain ongoing authorization package updates.
- Apply the Media Disposal Procedure to standardize system disposal practices.
- Audit all 10 partially implemented controls to finalize operational adoption.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

AREAS	STATUS MIX	SCORE	GAPS H · M · L
Prepare - organisation level	2 3 2	68%	2 0 3
Prepare - system level	2 3 5	70%	2 3 0
Categorize	1 3	88%	0 1 0
Select	2 2 2 1	75%	0 2 2
Implement	1 1 1	25%	2 1 0
Assess	1 2 4	86%	0 1 2
Authorize	1 2 1 2	42%	3 1 2
Monitor	3 1 2 2	59%	3 1 2

■ Not started
■ Planned
■ Partially implemented
■ Implemented, not evidenced
■ Implemented and evidenced
■ Not applicable

WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.

Today		66.2%
Evidence what already runs		71.6%
11 requirements		+5.4
Finish what is partly in place		81.4%
10 requirements		+9.8
Implement what is planned		96.1%
10 requirements		+14.7
Start what has not begun		100.0%
2 requirements		+3.9

DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.

Management Support Letter		3
Configuration Management Procedure		3
Change Management Policy		3
Risk Assessment and Treatment		2
Risk Assessment Report		2
Information Security Policy		2

All of these are in the NIST Risk Management Toolkit (54 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 2

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
I-2	Update control implementation information	Implement	IT Manager	Change Management Policy · Configuration Management Procedure
R-2	Risk analysis and determination	Authorize	Compliance Lead 21 Jan 2027	Risk Assessment Report · Risk Treatment Plan

HIGH Planned · 10

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
P-2	Risk management strategy	Prepare	Operations Manager 29 Oct 2026	Cyber Security Risk Management Framework · Risk Assessment and Treatment
P-6	Impact-level prioritisation	Prepare	IT Manager	
P-8	Mission or business focus	Prepare	Compliance Lead	
P-13	Information life cycle	Prepare	IT Manager	Data Retention Policy · Media Disposal Procedure +1 more
I-2b	Change control during build	Implement	To assign	Change Management Policy
R-4	Authorisation decision	Authorize	IT Manager 7 Jan 2027	Management Support Letter
R-5b	Conditions tracking	Authorize	To assign	
M-3	Ongoing risk response	Monitor	HR Manager	Vulnerability Management Policy · Incident Response Procedure
M-4	Authorisation package updates	Monitor	Operations Manager 26 Nov 2026	
M-6	Ongoing authorisation	Monitor	IT Manager 21 Jan 2027	

MEDIUM Partially implemented · 10

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
P-9	System stakeholders	Prepare	To assign	
P-10	Asset identification	Prepare	To assign	Asset Handling Policy

P-15	Requirements definition	Prepare	Risk Manager	Legal and Regulatory Requirements Procedure
C-3	Categorisation review and approval	Categorize	To assign	Management Support Letter
S-3	Control allocation	Select	Operations Manager 26 Nov 2026	Information Security Roles and Responsibilities
S-6	Plan review and approval	Select	HR Manager 12 Nov 2026	Management Support Letter
I-1	Control implementation	Implement	To assign	Configuration Management Procedure
A-6	Plan of action and milestones	Assess	Compliance Lead 21 Jan 2027	
R-1	Authorisation package	Authorize	Risk Manager 10 Dec 2026	
M-7	System disposal	Monitor	To assign	Media Disposal Procedure · Asset Handling Policy +1 more

LOW Implemented, not evidenced · 11

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
P-3	Risk assessment - organisation	Prepare	To assign	NIST 800-30 Risk Assessment Template · The Complete Guide to NIST 800-30 Risk Assessments +1 more
P-4	Organisationally-tailored control baselines and CSF profiles	Prepare	To assign	NIST CSF 2.0 Maturity Assessment Template
P-5	Common control identification	Prepare	To assign	Information Security Policy · Access Control Policy
S-2	Control tailoring	Select	To assign	
S-5	Continuous monitoring strategy - system	Select	To assign	Vulnerability Management Policy
A-4	Assessment reports	Assess	To assign	
A-5	Remediation actions	Assess	To assign	
R-3	Risk response	Authorize	To assign	Risk Assessment and Treatment · Risk Treatment Plan
R-5	Authorisation reporting	Authorize	To assign	
M-1	System and environment changes	Monitor	To assign	Change Management Policy · Configuration Management Procedure
M-5	Security and privacy reporting	Monitor	To assign	Information Security Policy

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com