

GOVERNANCE DOCS

FedRAMP (CR26)

Gap Assessment Report

FedRAMP Certification under the Consolidated Rules for 2026

Summit GovCloud Analytics (sample)

The analytics SaaS offering, its authorisation boundary and the supporting corporate services.

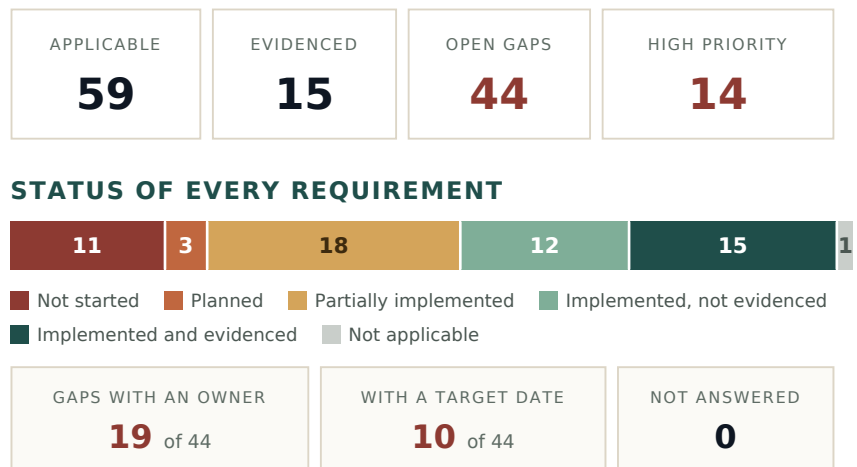
ASSESSED	25 September 2026
EDITION	Consolidated Rules for 2026, effective 4 July 2026
IN SCOPE	60 requirements, 59 applicable
PROFILE	Technology, software and SaaS · 10 to 49 people · FedRAMP PMO
PREPARED BY	Governance Docs

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 Summit GovCloud Analytics (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Summit GovCloud Analytics (sample) stands against FedRAMP



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 57.2% against FedRAMP across 59 applicable controls. 15 of them are implemented and evidenced.
- Most open gaps: Continuous monitoring and data sharing, with 8 at 48%. Strongest area: Architecture and service configuration at 86%.
- 12 controls are operating but not evidenced. Collecting their records alone lifts the score to 62.3% (+5.1 points), the cheapest gain available.
- 14 gaps are high priority (not started or only planned); 3 of them are in Policy, inventory and change management.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 3 high-priority gaps in Policy, inventory and change management	Operations Manager	Organizational Requirements Register
2	MEDIUM	Adopt and tailor the Certification Package Overview (+ JSON), which closes 4 open gaps	To assign	Certification Package Overview (+ JSON)
3	LOW	Evidence the 12 controls that already operate (+5.1 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

Your FedRAMP readiness stands at 57.2%, and you must prioritize establishing formal scope and authentication controls across 44 open gaps.

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

Our FedRAMP self-assessment shows an overall score of 57.2%, placing us at level 2 of 4, or Developing. While our architecture is strong, we face material exposures across 44 open gaps, including 14 high priority items in access control, recovery, and supply chain management. An auditor would identify these deficiencies today. To meet FedRAMP PMO expectations, leadership must assign owners to all open gaps, approve immediate remediation work, and authorize resources to complete foundational security documentation.

WHERE YOU STAND

The self-assessment places the organization at a developing readiness level of 2 of 4, with an overall score of 57.2%. Out of 59 applicable requirements, there are 44 open gaps, including 14 high priority gaps. While Architecture and service configuration scored highest at 86.1%, Recovery, incident, supply chain and training scored lowest at 37.5%. Currently, 11 requirements are not started, 3 are planned, 18 are partially implemented, and 12 are implemented but not evidenced. Only 19 gaps have assigned owners, and 10 have target dates.

WHAT IT MEANS FOR THE ORGANIZATION

The current operational pattern exposes the business to regulatory friction with the FedRAMP PMO. While technical architecture shows strength, critical governance disciplines lag behind. Key areas such as continuous monitoring, identity management, and incident recovery have multiple open gaps that an external assessor would identify. Operating without evidence for 12 implemented controls weakens credibility and inflates apparent risk. Furthermore, leaving more than half of all open gaps without assigned owners or target completion dates risks stalled remediation, potentially delaying authorization discussions and customer engagements.

WHERE TO FOCUS FIRST

Remediation should begin by defining the boundary through Minimum assessment scope and Security decision record. Immediate attention must also address high priority gaps in identity and incident recovery, specifically Passwordless or phishing-resistant authentication and Recovery plan and testing. Evidencing the 12 controls that are already implemented will raise the overall score to 62.3% with minimal effort. Assigning formal owners and deadlines to the remaining unassigned gaps ensures accountability across the team while stabilizing core compliance requirements.

1 · EXECUTIVE SUMMARY

PRIORITIES

PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1 Define assessment scope and record security decisions MAS Minimum assessment scope · SDR Security decision record	Lacking formal boundary definition leaves the organization unable to validate which systems are subject to FedRAMP PMO review. Completing these records establishes clear scope and prevents costly rework.	Draft the Minimum Assessment Scope Record to define core boundaries.	Minimum Assessment Scope Record FedRAMP Toolkit - 52 Templates for the FedRAMP Consolidated Rules 2026	30 DAYS
2 Implement phishing-resistant authentication and log review controls KSI-IAM-APM Passwordless or phishing-resistant authentication · KSI-MLA-ALA-RVL Log access and review	Identity, logging and monitoring stands at 50% with 7 open gaps, creating major operational security vulnerabilities. Failing to enforce strong authentication directly conflicts with regulator baselines.	Review authentication requirements and complete the Digital Identity Worksheet.	Identification and Authentication Policy (IA) FedRAMP Toolkit - 52 Templates for the FedRAMP Consolidated Rules 2026	30 DAYS
3 Establish recovery testing and supply chain risk policies KSI-RPL-ARP-TRC Recovery plan and testing · KSI-SCR-MIT-MON Supply chain risk	Recovery, incident, supply chain and training is the lowest-scoring area at 37.5%. Without tested contingency and vendor risk management, service disruption risks remain unmitigated.	Draft the Information System Contingency Plan to formalize recovery procedures.	Information System Contingency Plan FedRAMP Toolkit - 52 Templates for the FedRAMP Consolidated Rules 2026	60 DAYS
4 Establish continuous monitoring data sharing and access mechanisms CDS-TC Trust centre · CDS-PROG Programmatic access	Continuous monitoring and data sharing scored 47.5% with 8 open gaps. Operationalizing automated access and customer transparency is necessary for ongoing oversight.	Compile existing compliance records into a centralized Document Index.	Document Index FedRAMP Toolkit - 52 Templates for the FedRAMP Consolidated Rules 2026	90 DAYS

30 / 60 / 90-DAY ROADMAP

FIRST 30 DAYS - Assign accountable owners and completion target dates to all 44 open gaps. - Draft the Minimum Assessment Scope Record and the Security Decision Record. - Collect evidence for the 12 implemented controls to lift the score to 62.3%. - Adopt the Identification and Authentication Policy for phishing-resistant access controls.	DAYS 31 TO 60 - Draft and approve the Information System Contingency Plan and test recovery procedures. - Implement the Supply Chain Risk Management Policy across technology vendors. - Finalize the Configuration Management Plan to address redeployment controls. - Complete the Integrated Inventory Workbook to satisfy automated inventory requirements.	DAYS 61 TO 90 - Establish the customer trust centre and programmatic data sharing workflows. - Create the Document Index and finalize the machine-readable package components. - Complete privacy threshold analyses and related impact assessment documentation.
--	---	--

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
Start - path, class and type		70%	
Scope and certification package		50%	
Architecture and service configuration		86%	
Identity, logging and monitoring		50%	
Policy, inventory and change management		53%	
Recovery, incident, supply chain and training		38%	
Independent verification and validation		67%	
Continuous monitoring and data sharing		48%	

■ 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		57.2%
Evidence what already runs 12 requirements		62.3% +5.1
Finish what is partly in place 18 requirements		77.5% +15.2
Implement what is planned 3 requirements		81.4% +3.9
Start what has not begun 11 requirements		100.0% +18.6

DOCUMENTS THAT CLOSE THE MOST GAPS

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

Certification Package Overview (+ JSON)		4
Document Index		4
System and Communications Protection Policy (SC)		3
Configuration Management Plan		3
Identification and Authentication Policy (IA)		3
Vulnerability Detail Report (+ JSON)		3

All of these are in the FedRAMP 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 · 11

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

Ref	Requirement	Area	Owner · target	Closes it
MAS	Minimum assessment scope	Scope and certification package	Risk Manager	Minimum Assessment Scope Record
SDR	Security decision record	Scope and certification package	Compliance Lead	Security Decision Record (+ JSON)
KSI-IAM-APM	Passwordless or phishing-resistant authentication	Identity, logging and monitoring	Compliance Lead 21 Jan 2027	Identification and Authentication Policy (IA) · Digital Identity Worksheet
KSI-MLA-ALA-RVL	Log access and review	Identity, logging and monitoring	Operations Manager	Audit and Accountability Policy (AU)
KSI-PIY-RES-RIS	Executive support and security investment	Policy, inventory and change management	Operations Manager 4 Feb 2027	Organizational Requirements Register
KSI-CMT-RMV-RVP	Redeploy rather than modify	Policy, inventory and change management	To assign	Configuration Management Plan
KSI-RPL-ARP-TRC	Recovery plan and testing	Recovery, incident, supply chain and training	To assign	Information System Contingency Plan · Annual Assessment Plan
KSI-SCR-MIT-MON	Supply chain risk	Recovery, incident, supply chain and training	Compliance Lead	Supply Chain Risk Management Policy (SR)
CMU	Cryptographic module use	Recovery, incident, supply chain and training	IT Manager	System and Communications Protection Policy (SC)
CDS-TC	Trust centre	Continuous monitoring and data sharing	Risk Manager 10 Dec 2026	Document Index
CDS-PROG	Programmatic access	Continuous monitoring and data sharing	To assign	Document Index

HIGH Planned · 3

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

Ref	Requirement	Area	Owner · target	Closes it
KSI-PIY-GIV	Automated inventories	Policy, inventory and change management	To assign	Integrated Inventory Workbook (Excel)
IVV-USR-DUS	Sampling	Independent verification and validation	HR Manager	Security Assessment Plan
PRIV	Privacy documentation	Continuous monitoring and data sharing	To assign	Privacy Threshold Analysis · Privacy Impact Assessment +1 more

MEDIUM Partially implemented · 18

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

Ref	Requirement	Area	Owner · target	Closes it
START-CLASS	Certification class	Start	To assign	Certification Package Overview (+ JSON)
START-TYPE	Certification type	Start	To assign	How to Use This Toolkit (PDF)
START-CR26	CR26 adoption	Start	Compliance Lead	How to Use This Toolkit (PDF) · Toolkit FAQ (PDF)
JSN	Machine-readable package	Scope and certification package	HR Manager 21 Jan 2027	Certification Package Overview (+ JSON) · Security Decision Record (+ JSON) +1 more
KSI-CNA-MAT-RNT	Attack surface and network traffic	Architecture and service configuration	Risk Manager 29 Oct 2026	System and Communications Protection Policy (SC) · Configuration Management Plan
KSI-SVC-ASM	Key, certificate and secret management	Architecture and service configuration	Risk Manager 21 Jan 2027	System and Communications Protection Policy (SC)
KSI-MLA-EVC	Configuration evaluation	Identity, logging and monitoring	IT Manager	Configuration Management Plan
KSI-PIY-RVD	Vulnerability disclosure	Policy, inventory and change management	To assign	Vulnerability Detail Report (+ JSON)
KSI-RPL-RRO-ABO	Recovery objectives and backups	Recovery, incident, supply chain and training	Compliance Lead 24 Dec 2026	Information System Contingency Plan
KSI-INR-RIR	Incident response procedures	Recovery, incident, supply chain and training	To assign	Incident Response Policy (IR) · Incident Response Plan

SAMPLE REPORT - FICTIONAL ORGANISATION

IEC	Incident evaluation and communication	Recovery, incident, supply chain and training	Risk Manager 29 Oct 2026	Incident Report (+ JSON)
KSI-CED-RAT	Cybersecurity education	Recovery, incident, supply chain and training	HR Manager 29 Oct 2026	Awareness and Training Policy (AT)
IVV-AIA	Annual KSI assessment	Independent verification and validation	To assign	Key Security Indicators Register
CCM	Collaborative continuous monitoring	Continuous monitoring and data sharing	To assign	Ongoing Certification Plan · Ongoing Certification Report (+ JSON)
VDR	Vulnerability detection and response	Continuous monitoring and data sharing	IT Manager 24 Dec 2026	Vulnerability Detail Report (+ JSON)
VER	Vulnerability evaluation and reporting	Continuous monitoring and data sharing	IT Manager	Historical VER Activity Record (+ JSON) · Vulnerability Detail Report (+ JSON)
CDS-ACCESS	Access inventory and logging	Continuous monitoring and data sharing	To assign	Organizational Requirements Register
MKT	Marketplace listing	Continuous monitoring and data sharing	To assign	Certification Package Overview (+ JSON)

LOW Implemented, not evidenced · 12

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
CPO	Certification package overview	Scope and certification package	To assign	Certification Package Overview (+ JSON) · Document Index
SCG	Secure configuration guide	Scope and certification package	To assign	Secure Configuration Guide · User Guide
KSI-SVC-EIS	Security improvement	Architecture and service configuration	To assign	
KSI-IAM-AAM-ELP	Account management and least privilege	Identity, logging and monitoring	To assign	Access Control Policy (AC) · Identification and Authentication Policy (IA)
KSI-IAM-JIT	Just-in-time authorisation	Identity, logging and monitoring	To assign	Access Control Policy (AC) · Separation of Duties Matrix (Excel)
KSI-IAM-SNU-SUS	Non-user authentication and suspicious activity	Identity, logging and monitoring	To assign	Identification and Authentication Policy (IA) · Incident Response Plan

KSI-MLA-LET-OSM	Logging and SIEM	Identity, logging and monitoring	To assign	Audit and Accountability Policy (AU)
KSI-PIY-RSD	Security in the development lifecycle	Policy, inventory and change management	To assign	System and Services Acquisition Policy (SA)
SCN-EVA	Significant change classification	Policy, inventory and change management	To assign	Significant Change Notification (+ JSON)
IVV-ASSESSOR	FedRAMP Recognized assessor	Independent verification and validation	To assign	Independent Assessment Service Record
IVV-FIA	Annual independent assessment	Independent verification and validation	To assign	Annual Assessment Plan · Annual Assessment Report
IVV-SEI-SEE	Evidence of implementation and effectiveness	Independent verification and validation	To assign	Security Assessment Plan · Security Assessment Report

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