Accelerate FedRAMP with RegScale

Speed Time to Authorization with Continuous Controls Monitoring

Accelerate FedRAMP High package submission

18 months to **3** and reduce preparation time by **60%**

Accelerate Compliance and Savings

There's a better way to do compliance, and RegScale overcomes limitations in legacy GRC by bridging security, risk, and compliance through our Continuous Controls Monitoring (CCM) platform. Our CCM pipelines of automation, dashboards, and other tools deliver lower program costs, strengthen security, and minimize painful handoffs between teams. As the only CCM platform purpose-built on NIST OSCAL (Open Security Control Assessment Language), RegScale offers one-click exports to generate FedRAMP artifacts. OSCAL cuts down the time to final approval by being machine readable, preformatted, and validated with automated guidelines. Our CCM, OSCAL-native platform can accelerate initial package submission to as little as 3 months and reduce preparation time by 60%.

RegScale's Continuous Controls Monitoring Platform
allows companies to modernize and pivot from static compliance documentation and processes to a automated and scalable solution with more than 1,200 APIs and integrations.

CSPs (Cloud Services Providers)
become more efficient and effective in maintaining evidence, approval workflows, and change management — all things that cannot be done well in Excel spreadsheets or Word documents

Our ecosystem of technical integrations
streamline compliance and audit readiness, helping you meet and stay ahead of federal compliance requirements.

Our ecosystem of service providers
such as 3PAOs add value to the accelerated path to compliance and FedRAMP.

The Manual Way

- All different reports must be submitted as part of a flow to maintain FedRAMP certification.
- CSPs must maintain a POAM to track the identification of vulnerabilities through remediation on a monthly basis.
- Slow, painful, and cumbersome actions, largely due to manual processes of disparate parts.
- Too much paperwork steals time away from CSPs and federal agencies, leading to production and revenue loss.

Extreme Automation

- One-click export to OSCAL and generates FedRAMP artifacts.
- Automated POAM generation with the ability to output SAPs and SARs in OSCAL.
- Automation orchestrates manual compliance processes via thousands of integrations; and compliance as code makes FedRAMP turnaround times quicker.
- Self-updating paperwork and 60% reduction in preparation time.

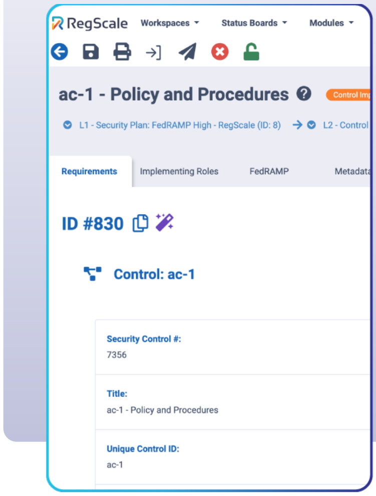
Time to Value in 4 Easy Steps

1 Create your Security Plan

2 Conduct Assessments

3 Export FedRAMP

4 Generate FedRAMP Artifacts



ac-1 - Policy and Procedures

L1 - Security Plan: FedRAMP High - RegScale (ID: 8) → L2 - Control

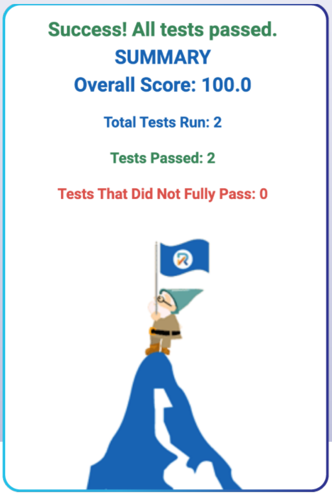
ID #830

Control: ac-1

Security Control #:
7356

Title:
ac-1 - Policy and Procedures

Unique Control ID:
ac-1

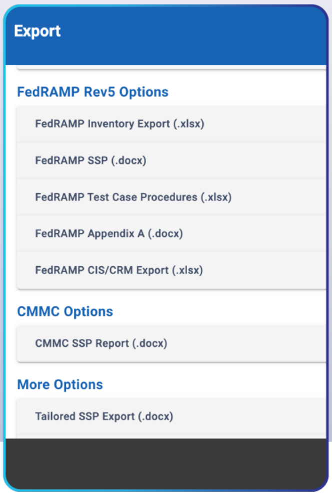


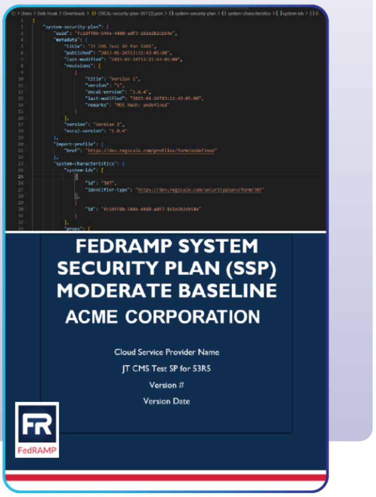
Success! All tests passed.
SUMMARY
Overall Score: 100.0

Total Tests Run: 2

Tests Passed: 2

Tests That Did Not Fully Pass: 0


Export
FedRAMP Rev5 Options
FedRAMP Inventory Export (.xlsx)
FedRAMP SSP (.docx)
FedRAMP Test Case Procedures (.xlsx)
FedRAMP Appendix A (.docx)
FedRAMP CIS/CRM Export (.xlsx)
CMMC Options
CMMC SSP Report (.docx)
More Options
Tailored SSP Export (.docx)



C: > Users > Dale Hoak > Downloads > {} OSCAL-security-plan-307 (2).json > {} system-security-plan > {} system-characteristics > [ ] system-ids > {} 0

```
{
    "system-security-plan": {
        "uuid": "fc1dff0b-544e-4480-adf7-161e1b2cb54e",
        "metadata": {
            "title": "JT CMS Test SP for 53R5",
            "published": "2023-01-24T13:21:43-05:00",
            "last-modified": "2023-01-24T13:21:43-05:00",
            "revisions": [
                {
                    "title": "Version 1",
                    "version": "1",
                    "oscal-version": "1.0.4",
                    "last-modified": "2023-01-24T13:21:43-05:00",
                    "remarks": "MD5 Hash: undefined"
                }
            ],
            "version": "Version 2",
            "oscal-version": "1.0.4"
        },
        "import-profile": {
            "href": "https://dev.regscale.com/profiles/form/undefined"
        },
        "system-characteristics": {
            "system-ids": [
                {
                    "id": "307",
                    "identifier-type": "https://dev.regscale.com/securityplans/form/307"
                },
                {
                    "id": "fc1dff0b-544e-4480-adf7-161e1b2cb54e"
                }
            ],
            "props": [
```

FEDRAMP SYSTEM SECURITY PLAN (SSP) MODERATE BASELINE
ACME CORPORATION

Cloud Service Provider Name
JT CMS Test SP for 53R5
Version #
Version Date

What is FedRAMP?

The Federal Risk and Authorization Management Program (FedRAMP), established in 2011, is a cloud-specific cybersecurity program for the federal government. Based on the FedRAMP Authorization Act, a “presumption of adequacy” ensures your FedRAMP ATO can be leveraged across multiple agencies. The U.S. government established the capability to approve cloudbased software for government use.

NIST OSCAL is a format that allows machine-to-machine communication and frees up the human to make risk-based decisions within the review loop. Reviews go from months to minutes when OSCAL is fully deployed at FedRAMP.

Ongoing Commitment

Under FedRAMP, organizations must engage in perpetual continuous monitoring of controls and regularly submit detailed vulnerability reports and asset inventories for the lifetime of the ATO.

To maintain certification, reports must be submitted to federal officials on a timely basis for continuous monitoring. FedRAMP touches everyone from revenue-generating CEOs to DevOps to engineering and federal sales.

Who Needs FedRAMP? The Impact

Based on the FedRAMP Authorization Act, signed into law on December 23, 2022, all cloud-based solutions procured by executive departments and agencies must be compliant with FedRAMP standards and maintain an authority-to-operate (ATO) status while in use. For a cloud solution provider to do business in this market, their cloud service offering (CSO) must be FedRAMP-authorized.

By the same token, FedRAMP needs the ability to take machinereadable packages and assess them with automation so it can accredit a lot more platforms faster

Accelerate your FedRAMP ATO journey with CCM today.

Ready to get started?

✉ sales@regscale.com | regscale.com