COMPASS ROSE
BY 360ADVANCED

GovRAMP

STEP-BY-STEP GUIDE TO ACHIEVING GovRAMP™ CERTIFICATION

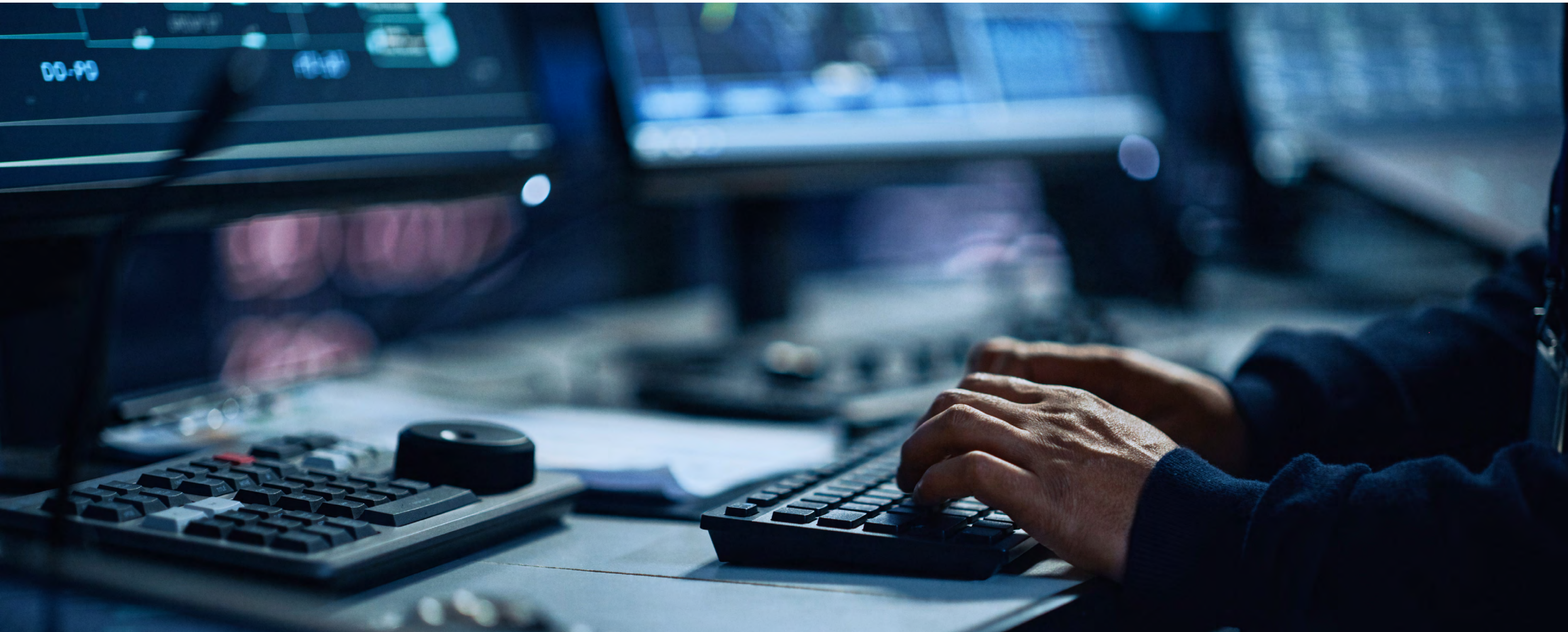
GovRAMP@360ADVANCED.COM | 360ADVANCED.COM | (866) 418-1708

Table of Contents

Introduction

GovRAMP (formerly called StateRAMP) is a cybersecurity framework designed to ensure that cloud service providers (CSPs) meet stringent cybersecurity standards for handling sensitive state and local government data. Modeled after the federal FedRAMP program, GovRAMP helps ensure that critical data is protected from cybersecurity threats by standardizing cloud security assessments.

Achieving GovRAMP certification is essential for any CSP wishing to work with government entities at the state level. This guide provides a step-by-step outline to help organizations navigate the GovRAMP certification process.



Step 1: Define the Context of Assessment Environment

The first step is always to understand the context of the assessment environment, then identify the data that is transmitted/stored/processed and the appropriate Data Classification and level of protection required (Low-Low+-Moderate-High) so that the Authorization Boundary is documented and understood.

- **Low:** For public, non-sensitive data that requires basic security controls
- **Low+:** For cloud services that handle a limited amount of sensitive data that requires enhanced security controls
- **Moderate:** For critical systems and confidential data that require comprehensive security controls
- **High:** For highly sensitive data and critical systems that require stringent control (equivalant to FedRAMP®)

Step 2: Conduct a Gap Analysis

A gap analysis is essential to understand where your organization's current security posture stands in relation to GovRAMP requirements.

- **Review current security controls** and policies against GovRAMP requirements.
- **Identify gaps** in your security framework that must be addressed to achieve certification.
- Work with your GovRAMP PMO or a third-party consultant to build a comprehensive roadmap to address these gaps.

Step 4: Develop a Plan of Action and Milestones (POA&M)

A POA&M will serve as your roadmap for addressing the security gaps identified during the gap analysis. The plan should include:

- **Actionable Steps** for addressing each gap or deficiency.
- **Timelines and milestones** for completing these actions.
- **Assigned responsibilities** to ensure accountability for each task.

Step 5: Implement Security Controls

Security controls should be implemented according to the required level of certification. Controls include:

- **User Access Control:** Restrict access to authorized users only.
- **Data Encryption:** Ensure all sensitive data is encrypted in transit and at rest.
- **Incident Response:** Develop a robust incident response plan to mitigate the impact of a potential cyber-attack.
- **Continuous Monitoring:** Implement tools and systems to monitor your environment continuously for threats and vulnerabilities.

At this stage, ensure compliance with **NIST SP 800-53** and other relevant standards.

Step 6: Conduct a Self-Assessment

Before engaging a third-party auditor, conduct a self-assessment to evaluate your readiness for certification:

- Use GovRAMP self-assessment templates to assess compliance with applicable controls.
- Address any remaining gaps or weaknesses identified during the self-assessment.

This step helps ensure that your organization is fully prepared for the formal audit process.

Step 7: Schedule a 3PAO Audit

For full GovRAMP certification, a Third-Party Assessment Organization (3PAO) must audit your security program. The audit will involve:

- **Preparation of documentation** demonstrating your compliance with GovRAMP security controls.
- **System and process reviews** conducted by the 3PAO.
- **Interviews and technical assessments** to validate your security practices.

Ensure that your team is fully prepared to provide evidence of compliance during the audit.

Step 8: Address Findings and Achieve Certification

Following the 3PAO audit, you may receive a list of findings or areas where improvements are required. Address these findings promptly:

- Submit evidence that demonstrates remediation of any identified issues.
- **Once all findings are addressed, you will be granted GovRAMP Authorized status.**

Your certification will be valid for a specific period, during which **ongoing compliance must be maintained.**

Step 9: Maintain Your Certification

GovRAMP certification is not a one-time effort. Continuous monitoring and regular assessments are required to maintain your certification status:

- **Conduct annual self-assessments** to ensure that your security practices remain compliant.
- **Plan for periodic recertification** with a 3PAO to maintain your authorized status.
- Keep up to date with evolving cybersecurity standards and emerging threats.

Pricing and Budgeting

The cost of achieving and maintaining GovRAMP certification can vary depending on several factors, including:

- **Company Size:** Larger organizations with more complex infrastructures tend to face higher audit costs.
- **Scope of the Audit:** The number of systems and environments being evaluated can influence pricing.
- **Pre-Audit Preparation:** Companies that invest in thorough gap analyses and remediation efforts may reduce overall audit costs.

Estimated Costs:

- Small organizations: $25,000 – $50,000
- Medium organizations: $50,000 – $100,000
- Large organizations: $100,000 and above

These costs may also include ongoing monitoring and re-certification expenses.

Conclusion

Achieving GovRAMP certification is critical for cloud service providers looking to engage with state and local government clients. By following this step-by-step guide, your organization can effectively prepare for and achieve GovRAMP certification, ensuring that you meet the necessary security requirements to protect sensitive government data.

For more information or assistance with your GovRAMP journey, contact 360 Advanced.

GovRAMP@360ADVANCED.COM

GovRAMP

COMPASS ROSE
BY 360ADVANCED