GovRAMP

NASPO
National Association of
State Procurement Officials

Procurement Cloud Security Resource Tool

Guiding SLED Organizations in Procurement Best Practices for Cloud Service Providers

AUGUST 2023

A PROCUREMENT TOOLKIT CREATED BY THE NASPO/GOVRAMP PROCUREMENT TASK FORCE

Table of Contents

ABOUT GOVRAMP

Founded at the beginning of 2020, GovRAMP was born from the clear need for a standardized approach to the cybersecurity standards required from service providers offering solutions to state and local governments.

GovRAMP is a registered 501(c)(6) nonprofit membership organization comprised of service providers offering IaaS, PaaS, and/or SaaS solutions, third party assessment organizations, and government officials. Our members lead, manage, and work in various disciplines across the United States and are all committed to making the digital landscape a safer, more secure place.

A PROCUREMENT TOOLKIT CREATED BY THE NASPO/GOVRAMP PROCUREMENT TASK FORCE

Cloud Procurement Frequently Asked Questions

What is the cloud?

Cloud refers to cloud computing solution provided by a service provider that delivers on demand computing services over the internet. As defined by the National Institute of Standards and Technology (NIST):

“Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

Cloud computing solutions are separated by the services provided for the cloud service model, such as software, platform, or infrastructure. Before undertaking cloud procurements, organizations must understand the service model to be acquired and the business objectives or challenges to be solved. The organization and service provider's responsibilities and contract terms and conditions will vary based on the service model and objectives.

What cloud services does procurement handle?

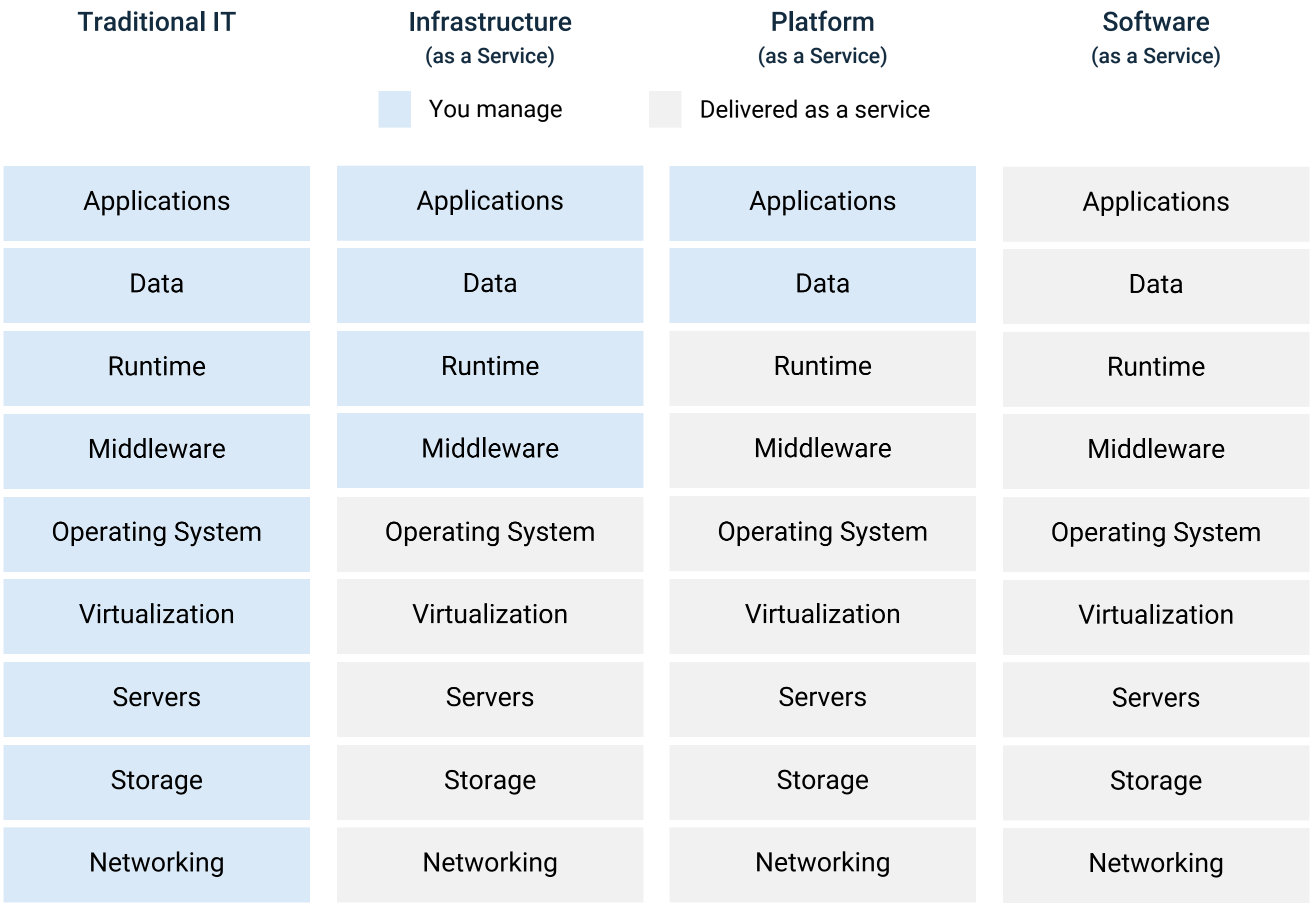
Procurement officials help organizations procure various cloud solutions, from web applications for email to platforms to develop and run custom-built software. Three common cloud services are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).

Software as a Service allows an organization to use a service provider's applications that run on a cloud infrastructure. Customers access the applications through web browsers or program interfaces. Platform as a Service allows an organization to run self-developed and acquired applications using programming languages and tools from a service provider. Infrastructure as a Service provides organizations the capability to provision processing, storage, networks, and computing resources to control and run applications and systems.

While the three services mentioned are common, various services are available in the cloud. These ever-evolving services put a finer point on the type of service provided. Still, each service typically fits within the three service models NIST defines. Procurement officials may see XaaS referenced, which refers to anything as a service; however, not all XaaS are cloud solutions. In addition, Cybersecurity as a Service (CSaaS) allows a third-party to monitor an organization's risk posture and provide expertise.

Does the type of cloud service shape a procurement?

Yes! Each cloud service model provides different services, which means organizations' and service providers' responsibilities will differ based on the service procured. The responsibility associated with each cloud service will require procurements of all types to be specific in the roles and responsibilities of each party.



🟦 You manage ⬜ Delivered as a service

Traditional IT	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
Applications	Applications	Applications	Applications
Data	Data	Data	Data
Runtime	Runtime	Runtime	Runtime
Middleware	Middleware	Middleware	Middleware
Operating System	Operating System	Operating System	Operating System
Virtualization	Virtualization	Virtualization	Virtualization
Servers	Servers	Servers	Servers
Storage	Storage	Storage	Storage
Networking	Networking	Networking	Networking

Guide to the Shared Responsibility Model

🟦 User's responsibility ⬛ Service Provider's responsibility

	Saas Dropbox, Salesforce CRM, Zoom, Microsoft 365, Google Workspace	Paas Microsoft Azure App Service, AWS Elastic Beanstalk, Google Kubernetes Engine, Red Hat OpenShift	Iaas Microsoft Azure, Amazon Web Services (AWS), Google Compute Engine (GCE)
Applications	⬛	🟦	🟦
Middleware	⬛	🟦	🟦
Virtualization	⬛	⬛	🟦
Data	⬛	⬛	🟦
O/S	⬛	⬛	🟦
Networking	⬛	⬛	🟦
Runtime	⬛	⬛	🟦
Servers	⬛	⬛	⬛
Storage	⬛	⬛	⬛

By integrating GovRAMP in their organizations, states can utilize GovRAMP template language for solicitations and contracts. Organizations must ensure that their contract clauses address data security and privacy. The Center for Digital Government published the Best Practice Guide for Cloud and As-A-Service Procurements. The guide contains a clause comparison matrix that offers a glimpse into the difference the cloud solution makes in the wording used. Organizations that have yet to implement GovRAMP, FedRAMP, or a RAMP program can find value in the Best Practice Guide for Cloud and As-A-Service Procurement.

Who is responsible for identifying data types?

Understanding data types is primarily the responsibility of those who work with data, such as data owners, software developers, data analysts, and database administrators. These professionals need to know how data is stored, processed, and transferred. However, it is critical that procurement professionals involve these data owners early in the procurement process.

Data owners handle data classification in liaison with other data professionals such as data analysts and database administrators. These individuals are responsible for organizing data into easily understood and used categories. For example, they might classify data based on its sensitivity (e.g., public or confidential) or type, such as customer information or sales data, HIPPA, or Privacy Data (personally identifiable information, PII).

By doing this, data professionals help ensure that the data is appropriately managed, protected, and utilized. This classification helps organizations make better decisions, protect sensitive information, and comply with legal and regulatory requirements.

Organizations can make more informed decisions that ensure their procurements align with organizational data strategies and mitigate potential data and privacy-related challenges by involving the data compliance officer to provide information on data requirements, quality standards, and potential data-related risks. The key objective is to have the appropriate business, security, and IT professionals involved at the conception phase of a potential procurement to identify the system, security, and data privacy requirements.

How does a vendor prove data security and privacy?

Vendors can provide assessments to organizations. Organizations must understand what they consider acceptable. Organizations can increase their cybersecurity maturity is to implement a RAMP program. Depending on what type of program an organization puts in place, it would determine whether they accept FedRAMP, GovRAMP, a third-party attestation, or a self-assessment by the vendor. Each option has its pros and cons, but there are many benefits to contracting with vendors who hold a FedRAMP or GovRAMP authorization. One benefit is that vendors must maintain and validate the security posture of their service offering(s) and have an annual assessment completed by a third-party assessment organization to retain an authorized status. The table below is an example of the types of assessment options available.

	GovRAMP	FedRAMP	Govt-Performed Audit	Third-Party Attestation	Self-Assessment
Based on NIST SP 800-53 Rev. 5	✓	✓	✓		
Requires annual audit by independent third-party assessment organization	✓	✓			
Requires monthly continuous monitoring	✓	✓			
Impact levels of low, moderate, and high	✓	✓	✓	✓	

Verified statuses of Ready and Authorized	✓	✓			
Available to any provider, regardless of federal contract status	✓		✓	✓	✓
Documentation available to federal, state, and local governments; public education institutions and special districts	✓			✓	
Centralized PMO reviews all security packages to ensure consistent application of standards and verification	✓				
Fast-track option for products with FedRAMP or GovRAMP	✓		✓		
Plans for mapping to other compliance frameworks: CJIS, MARSE, MMIS, IRS	✓		✓	✓	
Nonprofit mission to improve cyber posture for state and local government; education; special districts; and the providers who serve them	✓				

How do FedRAMP, GovRAMP, and RAMP programs differ?

FedRAMP (Federal Risk and Authorization Management Program) is a government-wide program that standardizes the security assessment, authorization, and continuous monitoring of cloud products and services. It provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by federal agencies.

GovRAMP (State Risk and Authorization Management Program) is similar to FedRAMP but tailored explicitly for state, local, tribal, and territorial government agencies. GovRAMP provides a standardized approach to cloud security assessment and authorization for state and local governments, enabling them to adopt cloud technologies more efficiently and securely.

RAMP (Risk and Authorization Management Program) is a broader term encompassing FedRAMP, GovRAMP, and similar national, state, or local programs. RAMP programs aim to streamline and standardize the security assessment and authorization processes for cloud products and services across various government entities, ensuring consistency and adherence to security standards.

How can procurement, data security, and privacy align?

Organizations can take the first step in aligning data security, privacy, and procurement by harmonizing procurement language and security policies, standards, and controls to eliminate conflicts and redundancies. In public procurements, general conditions, special conditions, requirements, and specifications are often layered into the solicitation package. When adopting new controls, reviewing other terms and conditions in the procurement is essential to avoid ambiguity and ensure the desired outcomes.

Adopting the most current version of NIST 800-53 as baseline controls for cloud services is another way organizations can align procurement, data security, and privacy. Avoiding customization, one-off controls, and incorporating a RAMP or RAMP service in cloud procurements will provide more substantial, manageable security measures. Providing clear and specific controls a service provider must conform to during the contract enables all parties to ensure data security and risk management remain a priority throughout the contract's life.

By changing the procurement infrastructure and acquisition policies and processes with cloud service governance and risk authorization and management practices, organizations can position themselves to procure services that fall within their risk tolerance. Piloting and implementing continuous monitoring by qualified auditors for cloud service control compliance protects the public's interest and enables organizations to use as-a-service solutions more securely.

What to include in a procurement for a cloud service?

The following solicitation checklist is from the Center for Digital Government Best Practice Guide for Cloud and As-A-Service Procurements, which can help organizations when procuring cloud services through solicitations as well as other procurement methods.

Solicitation Checklist

- □ What is the cloud security, data and privacy standards, and controls that the service provider must meet?
- □ What level of RAMP authorization (impact levels) must the service provider meet?
- □ What status level must the service provider product meet (GovRAMP pending, authorized, etc.)?
- □ When must the service provider achieve this status level?
- □ What is mandatory for compliance and what is subject to negotiations?
- □ What is the basis upon which the jurisdiction will consider exceptions?
- □ Has the solicitation been reviewed for redundancy and conflicts in terms and conditions and any security controls and requirements?
- □ Will resellers be eligible for awards?
- □ If resellers are eligible for awards, are there flow down requirements that will place sufficient compliance and performance obligations on the ultimate service provider providing the resold product or service?
- □ If resellers are eligible for an award, are they required to resell FEDRAMP and/or GovRAMP authorized offerings and, if so, does the authorization apply specifically to the cloud service products involved in the solicitation?
- □ Is there a process to negotiate terms and conditions with the service provider providing the product sold by the reseller?

Additional Resources

Center for Digital Government Best Practice Guide for Cloud and As-A-Service Procurements – Specifically, Appendix 7 Clause Comparison Matrix

NASPO

National Institute of Standards and Technology Glossary for IT definitions

GovRAMP

IRS 1075 - https://www.irs.gov/pub/irs-pdf/p1075.pdf

Payment Card Industry Data Security Standard (PCI DSS) - https://www.pcisecuritystandards.org/

Criminal Justice Information System (CJIS) - https://le.fbi.gov/cjis-division

Health Insurance Portability and Accountability Act (HIPAA) - https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html?language=es

Family Educational Rights and Privacy Act (FERPA) -
https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

European Union General Data Protection Regulation (GDPR) - https://gdpr-info.eu

GLBA (Gramm Leach Bliley Act) - https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Controlled Unclassified Information (CUI) - https://www.dodcui.mil/Policy/

Minimum Acceptable Risk Standards for Exchanges (MARS-E) - https://www.cms.gov/files/document/mars-e-v2-2-vol-1final-signed08032021-1.pdf

Data Classification Tool

Document Revision History

Date	Description	Version	Governance Body
December 2020	Original Updates	1.0	GovRAMP Steering Committee
October 2021	Security Status Updates	1.1	GovRAMP Staff
April 2022	Updates	1.2	GovRAMP Standards & Technical Committee and Board
August 2024	Updates to instructions and formatting	1.3	GovRAMP Staff

Introduction and Purpose

This document is intended to be used by state and local governments and procurement officials as a tool for determining the appropriate GovRAMP security requirements in procurements with the intent of procuring a service provider using or offering Infrastructure as a Service (IaaS), Software as a Service (SaaS), and/or Platform as a Service (PaaS) solutions that process, store, and/or transmit government data and any related information as defined by NIST 800-53, These include Personally Identifiable Information (PII), Personal Health Information (PHI), Payment Card Industry (PCI), and Criminal Justice Information (CJI). Identifying the data classification aids the Member Organization (Organization) in maintaining the security, confidentiality and integrity of their data in alliance with its governing body.

According to the Federal Information Security Management Act (FISMA) requirements, there are three distinct security objectives for information and information systems: confidentiality, integrity, and availability. These standards are used as the foundation to ensure vendors are providing solutions that meet the minimum-security requirements to process, store, and transmit certain types of government data and any related information.

It is necessary for the Organization, as defined by the GovRAMP Bylaws, to accurately determine their required security baseline prior to publishing a procurement so that the Organization can select a vendor that meets the government's needs and provides the appropriate security controls to protect the government data. The determination to which procurements this process should apply should be based on the Organization's policies and/or standards. Procurement should partner with the information security team, Chief Information Officer, and Chief Information Security Officer and/or the Risk Management team to ensure the appropriate standards are included in the procurement.

This data classification self-assessment is based on the NIST 800-53 Revision 5 (or current) requirements and designed to help state and local governments easily identify the appropriate GovRAMP security category to include a solicitation. Definitions of GovRAMP Ready, GovRAMP Provisionally Authorized, and GovRAMP Authorized, as well as Low Impact, Moderate Impact, and High Impact, can be found in the GovRAMP Security Assessment Framework located here, with further information available on GovRAMP's Templates and Resources page.

Instructions

Answer the questions in the survey section to determine what GovRAMP security category requirements you need to include in your solicitation to ensure your data is protected.

Survey Questions

1. Will the vendor process, transmit, and/or store non-sensitive State data, metadata, and/or data that may be released to the public that requires no additional levels of protection?
    a. If yes, GovRAMP Low is recommended.
2. Will the vendor process, transmit, and/or store personally identifiable information (PII) as defined by the U.S. Department of Labor (DOL)?
    a. If yes, GovRAMP Moderate is recommended.
3. Will the vendor process, transmit, and/or store protected health information (PHI) as defined by the Health Insurance Portability and Accountability Act (HIPAA)?
    a. If yes, GovRAMP Moderate is recommended.
4. Will the vendor process, transmit, and/or store payment card industry (PCI) data as defined by the PCI Security Standards Council (PCI SSC)?
    a. If yes, GovRAMP Moderate is recommended.

5. Will the vendor process, transmit, and/or store criminal justice information (CJI) data as defined by FBI CJIS division?
    a. If yes, GovRAMP Moderate is recommended.
    b. Note: States may add additional controls to GovRAMP Moderate to comply with the CJIS requirements.

6. Will the loss or unavailability of the data processed, transmitted, and/or stored by the service provider disrupt government operations?
    a. If yes, GovRAMP Moderate is recommended.

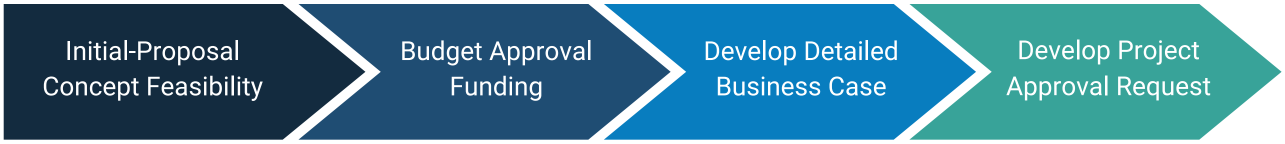
7. Will the loss or unavailability of the data that is processed, transmitted, and/or stored by the service provider result in a loss of confidence or trust in the government?
    a. If yes, GovRAMP Moderate is recommended.

Next Steps

Data processed, transmitted, and/or stored by the vendor includes information shared inside and outside of the provider's cloud service application. Similarly, if state or local laws have identified any other data type not included in the survey above as confidential, a GovRAMP Moderate is recommended. Once a procurement has been completed partner with the information security team, Chief Information Officer, Chief Information Security Officer, and/or Risk Management team to ensure the appropriate standards have been met.

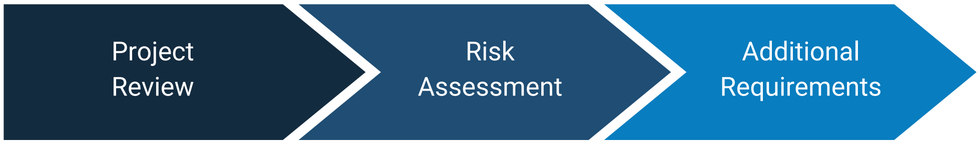
NIST 800-53 and Cloud Procurement: Process Flows

Project Inception


Initial-Proposal Concept Feasibility
Budget Approval Funding
Develop Detailed Business Case
Develop Project Approval Request

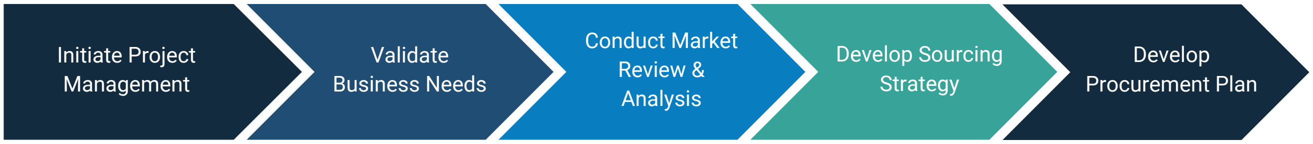
- Business case starts with a project request identifying the business mission and goal the need fulfills including background, outcome, business, involved personnel and system requirements, data inventory, data classification and risks.
- This will include any known business standards and compatibility that the system must meet.
- This should include an outcome statement about what the agency needs to address their business challenge - not a prescriptive design.
- This work, managed under the business sponsor who initiates the project includes participation from the knowledgeable SMEs.

Governance Review & Compliance



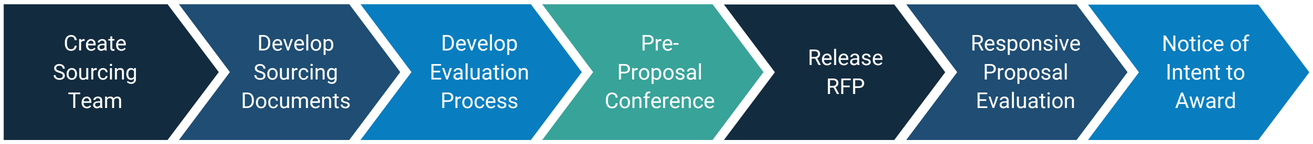
- Review and approval/disapproval of the cloud service provider (CSP) based project for compliance with enterprise architecture (EA) and security standards and policy.
- Documents completed in this step include approved project request with any additional requirements and a risk assessment with State RAMP Impact level and/or Security Snapshot.
- During pre-procurement risk assessment:
  - Verify or identify data classifications included in project.
  - Validate or determine appropriate GovRAMP Impact Level Classification (Low/Moderate/High) using GovRAMP Data Classification tool, and other specific requirements such as time deadlines for the work, Security Snapshot requirements, etc. based on data classification.
  - No projects can be procured without this review step to address compatibility, privacy standards, security standards, NIST 800-53 controls and other critical information essential to the procurement solicitation and successful contract execution.
- This can often be an iterative process between the governance review authority, requesting agency, Chief Information Security officer (CISO), Data Compliance Officer, appropriate SMEs and other identified stakeholders.

Sourcing Planning & Strategy


Initiate Project Management
Validate Business Needs
Conduct Market Review & Analysis
Develop Sourcing Strategy
Develop Procurement Plan

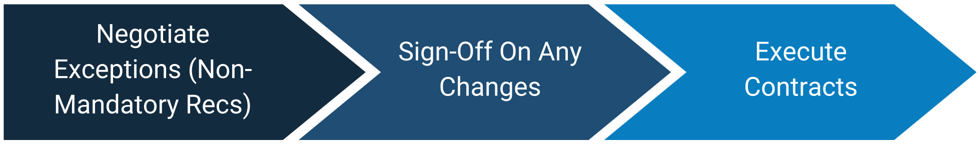
- At this point the project package has been approved and is ready for formal procurement planning.
- The approved project package now includes appropriate requirements for Enterprise Architecture, Cybersecurity, Privacy, NIST Controls, GovRAMP Impact Level, and project timelines to allow a procurement team and appropriate SMEs to develop a procurement plan and sourcing strategy.
- Documents completed in this step include; project charter, refined and validated business needs, market analysis, sourcing strategy and sourcing plan designed to address client, governance and market constraints and conditions and result in the identified outcomes for the project.
- The plan will identify the sourcing method (RFP, competitive proof of concept, cooperative purchase, multiple awards, pre-qualification, limited competition, etc.).

Sourcing Execution


Create Sourcing Team
Develop Sourcing Documents
Develop Evaluation Process
Pre-Proposal Conference
Release RFP
Responsive Proposal Evaluation
Notice of Intent to Award

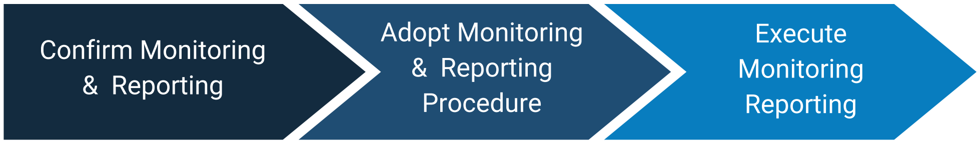
- Once the sourcing strategy and procurement plan are complete, reviewed and approved by the business owner, CISO and other key stakeholders, the source selection phase can begin.
- This phase creates the sourcing documents, selection process, evaluation process that align and harmonize with the procurement plan and when implemented help achieve the procurement strategy.
- In this phase the best qualified cloud service provider/s who meet the government's expectations for security, privacy and compliance with selected NIST 800-53 baseline controls are selected for contract award.
- For further reference see Solicitation Checklist for GovRAMP certification at the end of this document.

Contract Award Process



- This will vary depending on the sourcing method (RFP, cooperative contract, master agreement, etc.).
- Most contract steps will use standard clauses but aligned to the sourcing method and GovRAMP category impact level defined in the sourcing strategy.

Continuous Monitoring


Confirm Monitoring & Reporting
Adopt Monitoring & Reporting Procedure
Execute Monitoring Reporting

- This flow initiates continuous monitoring for the appropriate NIST 800-53 controls throughout the contract's life.
- Confirm monitoring and reporting requirements with provider including:
  - Confirm roles and responsibilities for reporting and monitoring,
  - Identify contacts
  - Identify timelines and key dates
  - Obtain authorizations and disclosure restrictions,

- Other information is required by the contract.
    - Adopt Monitoring and Reporting procedures to clarify and document the responsibilities of the party.
- Begin monitoring and reporting.

Solicitation Checklist for GovRAMP Certification

- Solicitation documents and/or selection documents clearly set out:
    - GovRAMP Impact Level product certification (Ready, Authorized, Provisionally Authorized) including NIST control baseline (Low, Low+, Moderate, or High) as appropriate for the provider service/s sought.
    - The time when the appropriate Impact Level must be achieved (fixed date, or amount of time).
    - When appropriate, GovRAMP Progressing Security requirement (reports, timelines).
    - Identify proof required to validate certifications for Impact Levels and Snapshot requirements.
    - Include requirements for continuous monitoring and reporting to the contracting officer or representative that include:
        - access to GovRAMP 3PAO reports,
        - required notice to the contracting officer for any change in Impact Level Status,
        - receipt of reports,
        - non-disclosure requirements,
        - provider's cooperation in developing a monitoring and reporting procedure, and
        - other items to create a workable and accountable process for timely reporting of providers change in compliance with selected NIST 800-53 baseline controls.
    - Remedies to address noncompliance with required baseline controls and loss of Impact Level status.
- Form a sourcing team and evaluation committee with representatives of the client agency, CISO, CIO and other key government stakeholders.
- Identify mandatory GovRAMP, security and privacy requirements that are not subject to exception and will be grounds for rejection as non-responsive.
- Develop a process to address exceptions to non-mandatory requirements in the RFP.
- Require mandatory submission of GovRAMP Impact Level certification, and/or official GovRAMP 3PAO, or Security Snapshot report (if required) with the proposal. This third-party report will be by the Contracting Officer to validate the products are compliant with NIST 800-53 baseline controls and responsive to the RFP.
- Minimize overlap and default to standard NIST 800-53 baseline controls by reviewing security, privacy and GovRAMP language in solicitation documents.

GovRAMP Standard Draft Policy Language

State/Entity __________ Draft Policy Language

1. Purpose

a. This policy is intended to address risk and protect privacy in State/ Entity ______ government information systems through a standardized and reusable approach based on controls derived from NIST 800-53, Rev 5, or most current controls to acquire commercially offered cloud products and services such as Infrastructure-as-a-Service, Platform-as-a-Service, and Software-as-a-Service that host information systems or applications operated by an agency or on behalf of an agency by a contractor or other organization.

b. The policy is further intended to promote standardization in procurement, contract management, compliance monitoring and foster contract competition among cloud-based service offerors progressing toward obtaining validated NIST 800-53 Rev 5 controls.

c. The goal of this policy is to eventually contract with providers whose cloud-based products and services offering have achieved a GovRAMP security status at the appropriate baseline control level determined by the State/Entity _____.

2. Policy

RISK MANAGEMENT ASSESSMENT AND PROCUREMENT

a. The State/Entity _____ requires an independent 3rd party attestation of the presences of NIST 800-53 Rev 5, or most current version, specifically through GovRAMP, for cloud-based information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information containing confidential or proprietary data (as defined in Section XXX) through a contract with an agency of State/Entity _______.

b. At a minimum, a current GovRAMP Security Snapshot must be provided prior to contract award. and GovRAMP Ready status must be achieved and documented within 12 months of the contract award. GovRAMP Authorization status shall be achieved and documented within 18 months of the award. A GovRAMP Security Snapshot must be maintained, to include monthly progress reporting until GovRAMP Ready Status is achieved. GovRAMP Security Snapshot monthly progress reporting should indicate progression toward GovRAMP Ready status.

c. Should the jurisdiction choose to accept a GovRAMP Provisionally Authorized status in lieu of Authorized status, service providers must provide proof of its Provisionally Authorized status to the jurisdiction at the time that the contract is awarded.

d. Nothing in this policy prevents State/Entity ________ from contracting for cloud-based product offering and service that are certified as GovRAMP Authorized when circumstances warrant and at least three (3) qualified providers meet the requirements.

3. Exceptions

a. This policy applies to all contracts for commercially available cloud-based product and service offerings as defined in this policy except:

   a. Ancillary services whose compromise would pose a negligible risk to government information or information systems, such as systems that make external measurements or read information from other publicly available services.
   b. Publicly available social media or communications platforms governed under State/Entity ____________social media policies, in which State/Entity _______ employees or support contractors may or may not enter State/Entity _________ information.
   c. Publicly available services that provide commercially available information.
   d. Existing contracts are awarded before adoption of the policy. Existing contracts for cloud-based products and services will be brought into compliance upon renewal, or when replaced with compliant contracts upon expiration at the discretion of the State/Entity _________ CISO.
   e. Other exceptions as determined by the State / Entity CISO (Or appropriate policy level position or entity)

b. All exceptions are considered policy deviations and may be granted in accordance with applicable law by the ___ (CISO/alternative) ___ or designee. Administrative, physical, or technical requirements may indicate the need for exemption from this Policy, for specific matters.

c. Following an appropriate risk assessment, the __ (CISO/alternative) ___ or designee, can acknowledge and/or escalate exception requests. Exceptions will be timely documented in the system designated by the ___ (CISO/alternative) ___ for that purpose.

d. Requests for exceptions must use the appropriate form and be approved by the __ (business unit/lead) __ or designee, prior to submission. At a minimum, the request must document the following:

   a. the control for which the exception is needed;
   b. the business justification and impact of the exception;
   c. the additional risks identified as a result of exception implementation; and,
   d. the compensating controls that are planned or implemented to

e. All exceptions must be documented in accordance with this Policy. Exceptions must be reevaluated on a grouped and rolling annual basis, in January. Exceptions granted in the six (6)-month period preceding an evaluation period will first be revaluated during the next reevaluation period.

GovRAMP Procurement Solicitation Best Practices

Purpose

This language should be used in procurements where the organization’s third-party risk management policy is applicable. The guidance and proposed clauses below should implement and conform to the requirements as set forth in the organization’s policy. The proper clauses as required by the needs of this solicitation should be selected and added to provide guidance to the bidders/respondents as to the expectations they need to meet both during the solicitation process and following award and contract execution.

Please note, these are model clauses. The exact language that your organization chooses to implement will be dependent on your policies and the needs of your organization. Language will vary based on the type of procurement, as well as the selection process utilized in that procurement, the cloud product, risk, and/or other factors determined by your organization.

Instructions on Use

To deploy GovRAMP within an organization's procurement and contracting process, follow these steps:

1. Determine the appropriate level of cybersecurity maturity and compliance required for your solicitation by evaluating the scope of relevant data and nature of the cloud service product. (See Procurement Best Practice Toolkit Flow Chart for details.)
2. Select the corresponding guidance and clauses from the 'Accept,' 'Prefer,' or 'Require' sections, as well as the Additional Continuous Monitoring and Pre-Contract Requirements sections below to include in your solicitation documents. For ease of use, all clauses will be in traditional typeface, while guidance will be bolded in italics.
3. Ensure continuous monitoring clauses are incorporated into your contracts to maintain security compliance throughout the contract duration.
4. Communicate clearly with potential vendors about the expectations and requirements for GovRAMP compliance.

Guidance and Clauses

ACCEPT

Solicitation Clause

Use this clause when your organization accepts GovRAMP alongside other cybersecurity standards.

Cloud service products subject to RAMP authorization - The successful proposer's cloud service product offering(s) that collect, process, maintain, use, share, disseminate, or dispose of information containing or impacting confidential or proprietary government data must demonstrate compliance with either GovRAMP or FedRAMP at a Public Control Baseline of (Low, Moderate, or High), or HITRUST at a Level (X).

Continuous Monitoring: GovRAMP

Use this clause when the cloud service provider is relying on GovRAMP, including monthly continuous monitoring, to satisfy your organization's cybersecurity standard.

Continuous Monitoring - Products utilizing a GovRAMP security status to satisfy this cybersecurity standard, must maintain its status for the duration of the contract and must grant visibility and access through GovRAMP for continuous monitoring as requested.

PREFER

Use these clauses where your organization prefers GovRAMP compliance over other standards. You can choose to implement an evaluation point preference when utilizing proposal-based solicitations, or a simple preference in those cases where you are selecting products from a master contract.

Solicitation Clause

Use this clause where your organization prefers GovRAMP compliance in proposal-based solicitations.

Cloud service products subject to RAMP authorization - The successful proposer's cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with one of the standards accepted in accordance with the [Name of the Organization's Policy] policy. However, those proposers who hold a verified GovRAMP status of Ready, Provisionally Authorized, or Authorized at a Public Control Baseline of (Low, Moderate, or High) shall be awarded preference over other standards in accordance with the points matrix outlined below.

Continuous Monitoring: GovRAMP

Use this clause when the cloud service provider is relying on GovRAMP to satisfy your cybersecurity standard.

Continuous Monitoring - Products utilizing a GovRAMP security status to satisfy this cybersecurity standard must maintain its status for the duration of the contract and must grant visibility and access through GovRAMP for continuous monitoring as requested.

REQUIRE

Use these clauses where your organization requires GovRAMP compliance to meet your RAMP Policy.

Option A: Low Maturity Levels

Solicitation Clause

Use this clause when the market is in transition, and immediate NIST control compliance is not required.

Cloud service products subject to RAMP authorization – The successful proposer's cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with National Institute of Standards and Technology (NIST) Special Publication 800-53 (revision 5 or latest version) at the Impact Level specified below or be enrolled in the GovRAMP Progressing Snapshot Program until the product achieves GovRAMP (Ready/Provisionally Authorized/Authorized) at a Public Control Baseline of (Low, Moderate, or High).

Continuous Monitoring: GovRAMP Progressing Security Snapshot Program

Use this clause to obtain access to continuous monitoring and to set deadlines for achieving GovRAMP Ready/Authorized/Provisionally Authorized status.

Continuous Monitoring - Products without a GovRAMP status of Ready, Authorized, or Provisionally Authorized must enroll in the GovRAMP Progressing Security Snapshot Program, complete quarterly Snapshots, and provide monthly progress reporting to GovRAMP until GovRAMP Ready, GovRAMP Authorized, or GovRAMP Provisionally Authorized status is obtained. The requirements for this contract are outlined below. If the provider does not already have a GovRAMP status of Ready, Authorized, or Provisionally Authorized, the appropriate status must be achieved in the following timeframes: (1) GovRAMP Ready status at a Public Control Baseline of (Low, Moderate, or High) must be obtained not later than 12 months after execution of this contract; (2) GovRAMP Authorized or Provisionally Authorized status at a Public Control Baseline of (Low, Moderate, or High) must be obtained not later than 18 months after execution of this contract. Subsequent Security Snapshots should reflect progress toward increased security controls and GovRAMP status. [Organization Name] must be granted visibility and access through GovRAMP for progress reviews as requested.

Option B: Maturing Markets

Solicitation Clause

Use this clause for markets where competition exists between cloud service providers who have achieved GovRAMP Ready or Provisionally Authorized Status. You should select the Public Control Baseline (Low, Moderate, or High) necessary for your specific procurement/contract.

Cloud service products subject to RAMP authorization – The successful proposer’s cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with National Institute of Standards and Technology (NIST) Special Publication 800-53 (revision 5 or latest version), and must possess GovRAMP Ready status at the Public Control Baseline of (Low, Moderate, or High). A GovRAMP Verified Security Status of Provisionally Authorized or Authorized at the Public Control Baseline of (Low, Moderate, or High) must be achieved within [Time period defined within Organization’s policy] months of contract award.

Continuous Monitoring: GovRAMP Ready to Provisionally Authorized or Authorized

Use this clause when a validated and fully compliant cloud provider is needed but may begin at Ready and transition to Provisionally Authorized or Authorized status.

Continuous Monitoring - Products with GovRAMP Ready status must grant visibility and access through GovRAMP for continuous monitoring as requested. Once a product transitions from Ready to Provisionally Authorized or Authorized status, it must maintain its Provisionally Authorized or Authorized status for the duration of the contract. Government must be granted visibility and access through GovRAMP for continuous monitoring as requested.

Option C: Mature Markets

Solicitation Clause

Use this clause for markets where most cloud service providers have products with GovRAMP Provisionally Authorized or Authorized status. You should select the Public Control Baseline (Low, Moderate, or High) necessary for your specific procurement/contract.

Cloud service products subject to RAMP authorization – The successful proposer’s cloud service product offering(s) that collect, process, store, maintain, transmit, dispose, and/or could impact government data must demonstrate compliance with National Institute of Standards and Technology (NIST) Special Publication 800-53 (revision 5 or latest version), and must possess GovRAMP Provisionally Authorized or Authorized status at the Public Control Baseline of (Low, Moderate, or High). Proposer must provide proof of their GovRAMP status at time of proposal submission.

Continuous Monitoring: GovRAMP Provisionally Authorized or Authorized

Use this clause for products that need to maintain a specific GovRAMP status throughout the contract duration.

Continuous Monitoring - Products with a verified status of GovRAMP Provisionally Authorized or Authorized must maintain either a GovRAMP Provisionally Authorized or a GovRAMP Authorized status for the duration of the contract. Government must be granted visibility and access through GovRAMP for continuous monitoring as requested.

Additional Continuous Monitoring Language

Specify continuous monitoring requirements for the duration of the contract.
Continuous Monitoring – For any resulting award(s) and subsequent contract(s), the awarded contractor(s) will:

1. Grant access to continuous monitoring and reporting upon receiving award for GovRAMP Security Snapshot, GovRAMP Progressing Snapshot, Ready status, Provisionally Authorized status, and Authorized status throughout the life of the contract.
2. Comply with (insert jurisdiction) requests to review all Third-Party Assessment Organization (3PAO) audits, risk assessments, vulnerability assessments, and penetration tests of the contractor's environment.
3. Respond to all vulnerabilities discovered or changes in status by providing a mutually agreed upon timeframe to resolve the issue and/or implement a compensating control.
4. Submit a procedure acceptable to the contracting officer to guide notification, reporting, and remediation of any change in status or flaws discovered by a Third-Party Assessment Organization (3PAO).

Pre-Contract Requirements

Proof of compliance with the required GovRAMP security status, or Security Snapshot, is necessary to complete due diligence. Depending on the sourcing methodology, what the proof is and the point when it must be furnished may vary. The clauses below must harmonize with the GovRAMP compliance clause utilized above. The examples below describe the different times in the award process when due diligence may be completed.

Proof of Compliance at Time of Proposal

With some methods, proof of compliance with the required GovRAMP security status, or Security Snapshot, is necessary for the contracting officer to complete due diligence before proposals are scored.
The most typical RFP methodology requires a responsiveness determination before proposals are evaluated and scored. The RFP requires proof of mandatory requirements such as proof of GovRAMP Authorization or attainment of Security Snapshot to be submitted with the proposal.

Vendor must submit one of the following at the time of proposal submission as requested by (Insert Organization Name):

1. Proof of current GovRAMP Authorized status in the form of a GovRAMP Letter
2. Proof of current GovRAMP Ready status in the form of a GovRAMP Letter
3. Valid GovRAMP Security Snapshot Score and proof of enrollment in the GovRAMP Progressing Security Snapshot Program

Failure to submit the document(s) listed above at the time of proposal will result in a proposal being deemed non-responsive.

Proof of Compliance after Proposal Submission, but Prior to Contract Award

For other methods, proof of GovRAMP Compliance or Security Snapshot level may be delayed after evaluation but before contract execution.

Again, proof of compliance with the required GovRAMP security status, or Security Snapshot level is required for the contracting officer to complete due diligence, but in this case the proof is due before contracts are executed by the Contracting Officer. In these circumstances the solicitation (RFP for a single award, RFP for multiple awards, Challenge Procurement, etc.) may allow a maximum period of time for the Contracting Officer to accept the proof, or it may be left unspecified. This method allows prospective contractors more time to obtain compliance but should not be indefinite. This method can help stimulate competition in an immature market because it allows in process Authorizations and Snapshots to be completed.

Prospective contractors must submit one of the following in accordance with the requirements of the RFP when required by the Contracting Officer and before a final award may be executed.

1. Proof of current GovRAMP Authorized Status in the form of a GovRAMP Letter.
2. Proof of current GovRAMP Ready Status in the form of a GovRAMP Letter
3. Valid State RAMP Security Score and proof of enrollment in GovRAMP Progressing Security Snapshot Program.

Proof of Compliance Before Final Contract Execution

For other methods, including, but not limited to price agreements, umbrella contracts, indefinite quantity awards, work order contracts or cooperative proof of GovRAMP compliance may be delayed until final contracts are executed by the using agency. While award mechanisms may vary by organization, when the proof is required and who validates the proof must be specified in the solicitation document. The final validation can be made by the contracting officer in price agreements and similar award processes where the GovRAMP compliance and requirements are made part of the final award, or they may be differed to the using agencies to validate the proof of compliance and complete the due diligence for prequalification listings and cooperative procurement awards.

Delayed proof can maximize competition by allowing emerging technology solutions to obtain appropriate levels of compliance and allow awarded cloud service providers to improve their security compliance poster over time. This gives organizations more choices and better fits for cloud services needs over time.

Selected cloud product provider must submit one of the following in accordance with the requirements of the RFP when required before a final award may be executed.

1. Proof of current GovRAMP Authorized Status in the form of a GovRAMP Letter.
2. Proof of current GovRAMP Ready Status in the form of a GovRAMP Letter
3. Valid State RAMP Security Score and proof of enrollment in GovRAMP Progressing Security Snapshot Program.

GovRAMP

NASPO®
National Association of
State Procurement Officials