FedRAMP customer overview

An overview of ServiceNow’s FedRAMP cloud platform and frequently asked questions
Table of contents

Introduction .......................................................................................................................... 3
What is FedRAMP? .............................................................................................................. 3
The ServiceNow GovCommunityCloud environment ......................................................... 3
Frequently asked questions ................................................................................................. 4
What are the benefits of the ServiceNow GovCommunityCloud (GCC)? ......................... 4
What are the differences between ServiceNow’s FedRAMP and commercial data centers? .... 5
How does this affect the way instances can be used? .......................................................... 5
Is the offering authorized for DoD Impact Level 4? ............................................................. 6
Who can use ServiceNow’s FedRAMP GCC environment? ............................................... 6
Can non-federal customers use the GCC environment? ....................................................... 6
What is the United States Government (USG) Addendum? ............................................... 6
What is the FedRAMP Customer Responsibility Matrix? .................................................... 7
What are the obligations for using the FedRAMP environment? ....................................... 7
How is technical support provided for FedRAMP customers? .......................................... 7
Do your support team members have appropriate clearances? .......................................... 7
Can customers use products from the AppStore in their FedRAMP instance? .................. 7
Where can I find documentation about the ServiceNow FedRAMP environment? .......... 7
What if I have further questions? ....................................................................................... 7
Conclusion ......................................................................................................................... 7
Resources ............................................................................................................................ 8
Acronyms used .................................................................................................................. 8
Introduction

This document is for current and prospective ServiceNow customers whose needs may fall under FedRAMP requirements. It outlines the US government’s FedRAMP program and then presents information on ServiceNow’s offerings in this area in the form of frequently asked questions.

What is FedRAMP?

FedRAMP is the Federal Risk Management Authorization Program. Its purpose is to encourage the use of secure cloud services for government agencies. Any cloud service processing, storing, or transmitting government data must be approved for FedRAMP.

From https://www.fedramp.gov/about/:

“The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

“FedRAMP enables Agencies to rapidly adapt from old, insecure legacy IT to mission-enabling, secure, and cost-effective cloud-based IT.

“FedRAMP created and manages a core set of processes to ensure effective, repeatable cloud security for the government. FedRAMP established a mature marketplace to increase utilization and familiarity with cloud services while facilitating collaboration across government through open exchanges of lessons learned, use cases, and tactical solutions.”

The ServiceNow GovCommunityCloud environment

ServiceNow has a FedRAMP-authorized cloud platform for US government customers, made up of a specialized operating environment and application suite:

- **The ServiceNow FedRAMP Environment**
  - A Continental United States (CONUS)-based dedicated infrastructure (facilities, servers, databases, networking devices) to process, store, and transmit government information using a multi-instance architecture.

- **The ServiceNow Service Automation Government Cloud Suite**
  - A collection of natively integrated applications designed to support IT service automation, resource management and shared support services.

The ServiceNow Service Automation Government Cloud Suite was granted a Joint Authorization Board (JAB) Provisional Authorization to Operate (P-ATO) with a High system categorization on August 12, 2019 and was approved at the US Department of Defense Impact Level 4 on October 6, 2019.

This solution is known as the ServiceNow GovCommunityCloud, and is authorized for FedRAMP High and DoD Impact Level 4 data and workloads. The user community includes federal, state, local, and tribal governments along with regulated organizations that have a requirement to meet US federal government security standards.

Customers must demonstrate that they qualify for this environment by being validated through ServiceNow’s GovCommunityCloud (GCC) approval program.
Frequently asked questions

What are the benefits of the ServiceNow GovCommunityCloud (GCC)?

The ServiceNow FedRAMP GCC environment is a physically and logically separate environment at ServiceNow, offering all the security and functionality of the standard commercial offering, plus these additional benefits:

- Compliance with NIST SP 800-53 Revision 4 controls, per the FedRAMP High baseline
- Compliance with the DoD Impact Level 4 controls, per the DISA Cloud Computing SRG
- Full Disk Encryption (FDE) for data at rest as standard
  - This is an additional cost option in the commercial environment
- US citizen support and administration
- Simplified path to ATO
  - Agencies can leverage ServiceNow’s FedRAMP Provisional authorization to issue their own ATO
- **Continuous monitoring** by the FedRAMP Program Management Office (PMO)
  - Annual assessment and penetration test against FedRAMP Third Party Assessment Organization (3PAO) standards
  - Annual penetration test by FedRAMP 3PAO
Monthly deliverables to the FedRAMP PMO

- Vulnerability scans of operating system, database, and web applications
- Inventory
- Plan of action and milestones (POA&M)

Customer responsibility matrix (see question below)

- Part of the FedRAMP Control Implementation Summary worksheet
- Provides information on controls with shared responsibilities
- Guides customer actions needed for secure use of the ServiceNow FedRAMP cloud

Documentation Repository (Kiteworks - see question below)

- This provides access to all authorization package documents, annual assessment results and monthly continuous monitoring submissions

What are the differences between ServiceNow’s FedRAMP and commercial data centers?

- Apart from the differences listed above, security controls are generally implemented in the same manner in both commercial and federal environments. This simplifies management and operations.
- While functionality and application code are the same in both environments, there are some differences:
  - There can be a delay in the availability of a major version release in FedRAMP due to the JAB approval process.
  - Dedicated hardware is available as an option. However, unlike the commercial environment, this is not a pre-requisite for Full Disk encryption (FDE), which is included by default with all FedRAMP instances.
  - Some features are not currently available in FedRAMP:
    - Benchmarks
    - Document viewer
    - Instance data replication
    - ServiceNow Antivirus Program (SNAP)
    - ServiceNow mobile apps

How does this affect the way instances can be used?

There are some implications to the FedRAMP and commercial environments being physically separate:

- There can be no cloning of instances between commercial and FedRAMP clouds
  - Update sets can be used to migrate application changes from commercial to production environment and vice versa
- Code migration, such as in the team development functionality, does not span between commercial and FedRAMP environments
- Development, test, and production instances typically all reside within the FedRAMP cloud
  - This allows simple code migration/cloning between development, test, and production instances
  - There is some flexibility dependent on need
    - e.g. the development instance could be in the commercial cloud to allow non-U.S. citizens to be administrators in the instance
Is the offering authorized for DoD Impact Level 4?
Yes. The FedRAMP high and DoD Impact Level 4 (IL4) categories have similar requirements, and we have received the DOD Cloud Provisional Authorization.

Who can use ServiceNow’s FedRAMP GCC environment?
All federal agencies (and some associated organizations) are able to use our FedRAMP environment:
- US federal, state, local, and tribal government with registered .gov or .mil domain addresses
- Government consultants
- Federally funded research and development centers (FFRDCs)

Can non-federal customers use the GCC environment?
Approval for organizations other than US federal government entities or instrumentalities to access the GCC environment is solely at ServiceNow’s discretion. Such organizations must demonstrate that they qualify for this environment by being validated through ServiceNow’s GCC approval program. Specifically, any organization other than US federal government entities or instrumentalities must meet the following criteria before ServiceNow can consider provisioning such organizations in the GCC environment:
- The organization must demonstrate they have a requirement to meet US federal government security standards by contractually agreeing to the terms in the ServiceNow US government (USG) contract addendum.

Below are examples of US federal government data types, contract clauses, and security standards that may demonstrate that an organization other than US federal government entities or instrumentalities are required to be included in the ServiceNow GCC environment:
- International Traffic in Arms (ITAR)
- Covered Defense Information
- Controlled Unclassified Information (CUI)
- Department of Defense (DoD) Unclassified Controlled Nuclear Information (UCNI)
- Department of Energy (DoE) UCNI
- Criminal Justice Information (CJI)
- Department of Defense Impact Level Data (up to DoD Impact Level 4)
- FedRAMP Data (up to FedRAMP High)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP)
- Requirements imposed on organizations from US federal government agencies (i.e., Department of Homeland Security, Department of the Treasury, Office of the Comptroller of the Currency, Centers for Medicare and Medicaid Services, etc.)
- Federal Acquisition Regulation and agency supplement (e.g., DFARS) clauses

What is the United States Government (USG) Addendum?
This is part of the contract between ServiceNow and customers wishing to use the FedRAMP environment. The main points of the USG Addendum are:
- Administrative access to their ServiceNow instance(s) must be restricted solely to US citizens who have been adjudicated (security cleared)
- A chief information security officer (CISO) or equivalent must be designated
• Acceptable Use Policies must be in place
This is usually already in place if a customer is meeting FAR or DFAR requirements.

What is the FedRAMP Customer Responsibility Matrix?
Securing a ServiceNow instance and the data it contains is a joint responsibility between the customer and ServiceNow, the cloud service provider (CSP). While ServiceNow has its own obligations for securing the platform and infrastructure, the FedRAMP Customer Responsibility Matrix outlines the actions a FedRAMP customer needs to take to operate their instances securely.

What are the obligations for using the FedRAMP environment?
Eligible customers must sign the ServiceNow United States Government (USG) Addendum and also adhere to the recommendations in the Customer Responsibility Matrix.

How is technical support provided for FedRAMP customers?
This is managed on a 24x7x365 basis by our dedicated federal government customer support team. Customer requests are placed and managed through the HiWAVE portal.

Do your support team members have appropriate clearances?
Yes, all ServiceNow FedRAMP support staff are required to undergo a US government background check and are adjudicated by the federal government for a Public Trust designation.

Can customers use products from the AppStore in their FedRAMP instance?
Yes. However, products in the AppStore are not included in our FedRAMP authorization scope. Customers must request a desired product in HiWAVE and “accept the risk” that it is outside our FedRAMP scope. Once acquired, customers must perform their own analysis on the product to determine whether it meets their security needs.

Where can I find documentation about the ServiceNow FedRAMP environment?
All of our FedRAMP-specific security documentation is stored within the ServiceNow boundary on the Kiteworks repository. Agencies can request access through the FedRAMP Program Management Office (PMO) by using the FedRAMP Package Request Form, quoting:
• Package Name "ServiceNow Service Automation Government Cloud Suite"
• Package ID “F1305072116"

Requests should be sent to info@fedramp.gov, asking for the “FedRAMP High Authorization Package” in Kiteworks.

What if I have further questions?
Feel free to contact us via the HiWAVE service portal or your support account manager. This ensures that your queries are captured, prioritized, and routed immediately, without reliance on individual availability.

Conclusion
It is common for US government agencies to use a cloud service for their data processing and storage needs.

The ServiceNow GovCommunityCloud (GCC) environment has been specifically developed for the benefit of federal agencies and is FedRAMP Authorized. It allows them to provide their users with the services they need with the confidence that they are entrusting their data to a flexible and reliable system with high levels of security and proven track record.

**Resources**

There is a wealth of information available online in the following publicly accessible locations:

- [US Government FedRAMP site](#)
- [FedRAMP Documents](#)
- [ServiceNow Product Documentation](#)
- [ServiceNow Community Support](#)

Existing Customers can also access:

- [CORE (Compliance Operations and Readiness Evidence)](#)
- [Cloud Security Trust and Compliance Center](#)
- [General Technical Support](#)

**Acronyms used**

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Expanded Term</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATO</td>
<td>Authority to Operate</td>
</tr>
<tr>
<td>CSP</td>
<td>Cloud Service Provider</td>
</tr>
<tr>
<td>FAR</td>
<td>Federal Acquisition Regulation</td>
</tr>
<tr>
<td>DFARS</td>
<td>Defense FAR Supplement</td>
</tr>
<tr>
<td>JAB</td>
<td>Joint Authorization Board</td>
</tr>
<tr>
<td>P-ATO</td>
<td>Provisional ATO</td>
</tr>
<tr>
<td>USG</td>
<td>United States Government</td>
</tr>
<tr>
<td>FedRAMP</td>
<td>Federal Risk and Authorization Management Program</td>
</tr>
<tr>
<td>OCISO</td>
<td>Office of the Chief Information Security Officer</td>
</tr>
<tr>
<td>3PAO</td>
<td>3rd Party Assessment Organization</td>
</tr>
<tr>
<td>GCC</td>
<td>ServiceNow Government Community Cloud</td>
</tr>
</tbody>
</table>