FedRAMP Low or Moderate Control Implementation Summary (CIS) Workbook Template

Template Revision History

Date	Description	Version	Author
6/6/2014	Major revision for SP800-53 Revision 4. Included new template and formatting changes.	2.1	FedRAMP PMO
5/18/2016	Removed from Control Implementation Summary Template, deleted control CM-8 (2).	3	FedRAMP PMO
6/6/2017	Updated logo.	3.1	FedRAMP PMO
8/6/2020	Major revision. Updated Instructions worksheet, added second level of control detail to the CIS and CRM Worksheets, updated CIS Worksheet selections, revised CRM Worksheet approach and "Guidance" section, and updated Example CRM Worksheet Responses for the new approach.	4.0	FedRAMP PMO

System Name (CSP to complete all cells)

CSP	System Name	Impact Level
New Relic	New Relic Observability Platform	Moderate

Document Revision History (CSP to complete all cells)

Date	Description	Version	Author
8/6/2020	Initial Version New Template	1.0	Kratos for New Relic
8/17/2020	Updated older version into New Template	1.1	Kratos for New Relic
7/26/2021	2021 Annual Review	1.1	New Relic
6/3/2022	2022 Annual Review	1.2	Sapia for New Relic
7/18/2023	2023 Annual Review	1.3	New Relic

How to Contact Us

Questions about FedRAMP or this document should be directed to info@fedramp.gov. For more information about FedRAMP, visit the website at https://www.fedramp.gov.

About This Template and Who Should Use It

Cloud Service Providers (CSPs) must use this High Control Implementation Summary (CIS) Workbook Template to summarize a High system's implementation status for all controls and enhancements, and to identify and describe the customer Agency/CSP responsibilities. The CSP must submit the completed CIS Workbook as part of the system's final security authorization package, as System Security Plan (SSP) Attachment 9.

The audience for the completed CIS Workbook includes Third Party Assessment Organizations (3PAOs); customer Agencies and CSPs; and the FedRAMP Joint Authorization Board (JAB) and Program Management Office (PMO).

This workbook should be updated as part of a CSP's regular continuous monitoring activities.

Instructions

The CSP must complete two worksheets in this CIS Workbook Template: the FedRAMP High Control Implementation Summary (CIS) Worksheet, hereafter called the CIS Worksheet; and the FedRAMP High Customer Responsibility Matrix (CRM) Worksheet, hereafter called the CRM Worksheet. The remaining two worksheets (Instructions and Example CRM Worksheet Responses) provide information on completing the CIS and CRM worksheets.

Completing the CIS Worksheet

On the CIS Worksheet, enter an "X" to correspond to the selections for each control and control enhancement in the final, approved System Security Plan (SSP) for:

1) Implementation Status

"Implementation Status" refers to the implementation status of the control (e.g., Implemented, Partially Implemented, Planned, Alternative Implementation, N/A).

2) Control Origination

“Control Origination” refers to which entity has responsibility for implementing the control. The following table defines the control origination options.

Control Origination and Definition

Control Origination	Definition	Example
Service Provider Corporate	A control that originates from the CSP's corporate network.	Domain Name System (DNS) from the corporate network provides address resolution services for the information system and the service offering.
Service Provider System Specific	A control specific to a particular CSP system and the control is not part of the service provider corporate controls.	A unique host-based intrusion detection system (HIDS) is available on the service offering platform that is separate from the corporate network and dedicated to the service offering.
Service Provider Hybrid (Corporate and System Specific)	A control that makes use of both corporate controls and additional controls specific to a particular CSP system.	Corporate may provide scanning of the CSP's service offering utilizing the corporate network infrastructure, databases, or web-based applications.
Configured by Customer (Customer System Specific)	A control where the customer needs to apply a configuration to meet the control requirement.	User profiles, policy/audit configurations, enabling/disabling key switches (e.g., enable/disable http or https, etc.), entering an IP range specific to their organization that are configurable by the customer.
Provided by Customer (Customer System Specific)	A control where the customer needs to provide additional hardware or software to meet the control requirement.	The customer provides a Security Assertion Markup Language (SAML) Single Sign On (SSO) solution to implement two-factor authentication.
Shared (Service Provider and Customer Responsibility)	A control that is managed and implemented partially by the CSP and partially by the customer.	Security awareness training must be conducted by both the CSP and customer.
Inherited from Pre-Existing Authorization	A control that is inherited (by the CSP service offering) from another CSP system that has already received a FedRAMP Authorization.	A Platform as a Service (PaaS) or Software as a Service (SaaS) provider inherits Physical and Environmental Protection (PE) controls from an Infrastructure as a Service (IaaS) provider.

Completing the CRM Worksheet

To complete the CRM Worksheet, follow the instructions in the “Guidance” section at the top of the CRM Worksheet. The CRM Worksheet responses must clearly describe what the CSP provides to customer agencies and CSPs, and what responsibilities customers have for each control; therefore, it may also be necessary to reference the final, approved version of the SSP for customer responsibility details. Example CRM responses, for sample controls, are provided in the Example CRM Worksheet Responses sheet.

CSP:

The CRM should contain information for what a leveraging party needs to implement in order to obtain and maintain their ATO. The Customer responsibility outlines the remaining controls that need to be implemented by the leveraging entity for compliance. For example, if a CSP provides account management but not multifactor authentication, the CRM should include the provisioning responsibilities for creating accounts in AC-2 and should include the multifactor responsibilities in the IA-5 section of the CRM.

Leveraging Entity:

The leveraging entity should be able to analyze the CRM to define all the controls they will need to engineer, design, define and implement in order to be in compliance with the FedRAMP baseline.

3PAO:

The CRM will define the test cases need to verify the accuracy of the CRM. The testing of the CRM should validate the items that the leveraging entities will need to implement to maintain compliance with the FedRAMP baseline are accurate.

There could be many different services offered by CSPs that are included within the authorization boundary. CSPs are required to delinate customer responsibilities associated with each service.

FedRAMP Low or Moderate Control Implementation Summary (CIS) Worksheet

Control ID	Implementation Status					Control Origination						
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization
AC-01	x						x				x	
AC-02	x										x	
AC-02 (01)	x						x				x	
AC-02 (02)	x										x	
AC-02 (03)	x										x	
AC-02 (04)	x						x				x	
AC-02 (05)	x						x				x	
AC-02 (07)	x						x				x	
AC-02 (09)	x										x	
AC-02 (10)	x										x	
AC-02 (12)	x										x	
AC-03	x										x	
AC-04	x										x	
AC-04 (21)	x										x	
AC-05	x										x	
AC-06	x						x				x	
AC-06 (01)	x										x	
AC-06 (02)	x										x	
AC-06 (05)	x										x	
AC-06 (09)	x										x	
AC-06 (10)	x										x	
AC-07	x										x	
AC-08	x										x	
AC-10	x										x	x
AC-11	x										x	x
AC-11 (01)	x										x	
AC-12	x										x	
AC-14	x						x				x	
AC-17	x										x	
AC-17 (01)	x										x	
AC-17 (02)	x										x	x
AC-17 (03)	x										x	
AC-17 (04)	x										x	
AC-17 (09)	x										x	
AC-18	x											x
AC-18 (01)	x											x
AC-19	x										x	
AC-19 (05)	x										x	x
AC-20	x										x	
AC-20 (01)	x										x	
AC-20 (02)	x										x	
AC-21	x										x	
AC-22	x										x	
AT-01	x						x					
AT-02	x						x					
AT-02 (02)	x						x					
AT-03	x						x					
AT-04	x						x					
AU-01	x						x					
AU-02	x											
AU-02 (03)	x						x					
AU-03	x						x					
AU-03 (01)	x						x					
AU-04	x						x					
AU-05							x					
AU-06	x						x					
AU-06 (01)	x						x					
AU-06 (03)	x						x					
AU-07	x						x					
AU-07 (01)	x						x					
AU-08	x						x					
AU-08 (01)	x						x					
AU-09	x						x				x	
AU-09 (02)	x						x				x	
AU-09 (04)	x						x				x	
AU-11	x						x				x	
AU-12	x						x					
CA-01	x						x				x	
CA-02	x						x					
CA-02 (01)	x						x					
CA-02 (02)	x						x					
CA-02 (03)	x						x					
CA-03	x						x					
CA-03 (03)	x						x					
CA-03 (05)	x						x					
CA-05	x						x					
CA-06	x						x					
CA-07	x						x					
CA-07 (01)	x						x					
CA-08	x						x					
CA-08 (01)	x						x					
CA-09	x						x				x	
CM-01			x				x					
CM-02			x				x					
CM-02 (01)			x				x					
CM-02 (02)			x				x					
CM-02 (03)			x				x					
CM-02 (07)			x				x					
CM-03			x									
CM-04			x									
CM-05			x									
CM-05 (01)			x									
CM-05 (03)			x									
CM-05 (05)			x									
CM-06			x				x					x
CM-06 (01)			x				x					x
CM-07			x									x
CM-07 (01)			x				x					
CM-07 (02)			x				x					
CM-07 (05)			x				x					
CM-08			x				x					
CM-08 (01)			x				x					
CM-08 (03)			x				x					
CM-08 (05)			x				x					
CM-09			x				x					
CM-10			x				x					
CM-10 (01)			x				x					
CM-11			x				x					
CP-01			x				x					
CP-02			x				x				x	
CP-02 (01)			x				x				x	
CP-02 (02)			x									x
CP-02 (03)			x				x				x	
CP-02 (08)			x				x				x	
CP-03			x				x				x	
CP-04			x				x				x	
CP-04 (01)			x				x				x	
CP-06			x									x
CP-06 (01)			x									x
CP-06 (03)			x									x
CP-07			x									x
CP-07 (01)			x									x
CP-07 (02)			x									x
CP-07 (03)			x									x
CP-08			x									x
CP-08 (01)			x									x
CP-08 (02)			x									x
CP-09			x				x	x			x	x
CP-09 (01)			x				x					x
CP-09 (03)			x				x					x
CP-10			x				x					
CP-10 (02)			x				x					
IA-01	x						x				x	
IA-02	x										x	
IA-02 (01)	x										x	
IA-02 (02)	x										x	
IA-02 (03)	x											x
IA-02 (05)	x										x	
IA-02 (08)	x										x	
IA-02 (11)	x										x	
IA-02 (12)	x										x	
IA-03	x										x	
IA-04	x										x	
IA-04 (04)	x										x	
IA-05											x	x
IA-05 (01)	x										x	x
IA-05 (02)	x										x	
IA-05 (03)	x										x	
IA-05 (04)	x										x	
IA-05 (06)	x										x	x
IA-05 (07)	x										x	
IA-05 (11)	x										x	
IA-06	x										x	
IA-07	x										x	x
IA-08	x										x	
IA-08 (01)	x									x		
IA-08 (02)	x									x		
IA-08 (03)	x									x		
IA-08 (04)	x									x		
IR-01			x				x					
IR-02			x				x				x	
IR-03			x				x				x	
IR-03 (02)			x				x				x	
IR-04			x				x				x	
IR-04 (01)			x				x				x	
IR-05			x				x				x	
IR-06			x				x				x	
IR-06 (01)			x				x				x	
IR-07			x				x				x	
IR-07 (01)			x				x				x	
IR-07 (02)			x				x				x	
IR-08			x				x				x	
IR-09			x				x				x	
IR-09 (01)			x				x				x	
IR-09 (02)			x				x				x	
IR-09 (03)			x				x				x	x
IR-09 (04)			x				x				x	x
MA-01	x						x					
MA-02	x											x
MA-03	x											x
MA-03 (01)	x											x
MA-03 (02)	x											x
MA-03 (03)	x											x
MA-04	x											x
MA-04 (02)	x						x					x
MA-05	x											x
MA-05 (01)	x											x
MA-06	x											x
MP-01	x						x					
MP-02	x											x
MP-03	x											x
MP-04	x											x
MP-05	x											x
MP-05 (04)	x											x
MP-06	x											x
MP-06 (02)	x											x
MP-07	x											x
MP-07 (01)	x											x

FedRAMP Low or Moderate Control Implementation Summary (CIS) Worksheet

Control ID	Implementation Status					Control Origination						
	Implemented	Partially Implemented	Planned	Alternative Implementation	N/A	Service Provider Corporate	Service Provider System Specific	Service Provider Hybrid (Corporate and System Specific)	Configured by Customer (Customer System Specific)	Provided by Customer (Customer System Specific)	Shared (Service Provider and Customer Responsibility)	Inherited from Pre-Existing Authorization
PE-01	x						x					
PE-02	x											x
PE-03	x											x
PE-04	x											x
PE-05	x											x
PE-06	x											x
PE-06 (01)	x											x
PE-08	x											x
PE-09	x											x
PE-10	x											x
PE-11	x											x
PE-12	x											x
PE-13	x											x
PE-13 (02)	x											x
PE-13 (03)	x											x
PE-14	x											x
PE-14 (02)	x											x
PE-15	x											x
PE-16	x											x
PE-17	x											x
PL-01	x						x					
PL-02	x						x				x	
PL-02 (03)	x						x				x	
PL-04	x						x				x	
PL-04 (01)	x						x				x	
PL-08	x						x				x	
PS-01	x							x				
PS-02	x						x				x	
PS-03	x					x					x	
PS-03 (03)					x		x					
PS-04	x						x				x	
PS-05	x						x				x	
PS-06	x						x				x	
PS-07	x						x				x	
PS-08	x						x				x	
RA-01			x				x					
RA-02			x				x				x	
RA-03			x				x				x	
RA-05			x				x					
RA-05 (01)			x				x					
RA-05 (02)			x				x					
RA-05 (03)			x				x					
RA-05 (05)			x				x					
RA-05 (06)			x				x					
RA-05 (08)			x				x					
SA-01	x						x					
SA-02	x						x				x	
SA-03	x						x					
SA-04	x										x	
SA-04 (01)	x										x	
SA-04 (02)	x										x	
SA-04 (08)	x										x	
SA-04 (09)	x										x	
SA-04 (10)	x									x		
SA-05	x										x	
SA-08	x						x					
SA-09	x						x					
SA-09 (01)	x						x					
SA-09 (02)	x						x					
SA-09 (04)	x						x					
SA-09 (05)	x						x					x
SA-10	x						x					
SA-10 (01)	x						x					x
SA-11	x						x					
SA-11 (01)	x						x					
SA-11 (02)	x						x					
SA-11 (08)	x						x					
SC-01	x						x					
SC-02	x						x					
SC-04	x						x					
SC-05	x						x					
SC-06	x						x					x
SC-07	x						x				x	
SC-07 (03)	x						x				x	
SC-07 (04)	x						x				x	
SC-07 (05)	x						x				x	
SC-07 (07)	x						x					x
SC-07 (08)	x						x					
SC-07 (12)	x						x					
SC-07 (13)				x			x					x
SC-07 (18)	x						x					
SC-08	x						x				x	x
SC-08 (01)	x						x					
SC-10	x										x	x
SC-12	x						x				x	x
SC-12 (02)	x						x				x	
SC-12 (03)	x						x				x	
SC-13	x						x					x
SC-15	x						x					
SC-17	x						x				x	
SC-18	x						x					
SC-19	x						x					x
SC-20	x						x					
SC-21	x						x					
SC-22	x						x					
SC-23	x						x				x	
SC-28	x						x					
SC-28 (01)	x						x					
SC-39	x						x					
SI-01	x						x					
SI-02	x						x					
SI-02 (02)	x						x					
SI-02 (03)	x						x					
SI-03	x						x					
SI-03 (01)	x						x					
SI-03 (02)	x						x					
SI-03 (07)	x						x					
SI-04	x						x					
SI-04 (01)	x						x					
SI-04 (02)	x						x					
SI-04 (04)	x						x					
SI-04 (05)	x						x					
SI-04 (14)	x						x					x
SI-04 (16)	x						x					
SI-04 (23)	x						x					
SI-05	x						x				x	
SI-06	x						x					
SI-07	x						x					x
SI-07 (01)	x						x					
SI-07 (07)	x						x					
SI-08					x		x					
SI-08 (01)					x		x					
SI-08 (02)					x		x					
SI-10	x						x					
SI-11	x						x					
SI-12	x						x					
SI-16	x						x					

FedRAMP Low or Moderate Customer Responsibility Matrix (CRM) Worksheet

GUIDANCE:

• Refer to CSP responses in the completed CIS Worksheet, "Control Origination" section.

• For Control IDs identified in the CIS Worksheet as Service Provider Corporate, Service Provider System Specific, or Service Provider Hybrid (Corporate and System Specific), enter "Yes" in the "Can Be Inherited from CSP" column below and leave the "Specific Inheritance and Customer Agency/CSP Responsibilities" column blank.

• For Control IDs identified in the CIS Worksheet as Shared (Service Provider and Customer Responsibility), enter "Partial" in the "Can Be Inherited from CSP" column below. In the "Specific Inheritance and Customer Agency/CSP Responsibilities" column, describe which elements are inherited from the CSP and describe the customer responsibilities.

• For Control IDs identified in the CIS Worksheet as Configured by Customer (Customer System Specific) or Provided by Customer (Customer System Specific), enter "No" in the "Can Be Inherited from CSP" column below. In the "Specific Inheritance and Customer Agency/CSP Responsibilities" column, explain why the Control ID cannot be inherited, and describe the customer responsibilities.

• For CSPs that offer a variety of services or features, the CSP must clearly describe any customer responsibilities associated with each service or feature, in the "Specific Inheritance and Customer Agency/CSP Responsibilities" column, for each affected control and must clearly link the responsibilities to the service or feature. CSPs with multiple services or features may wish to add a key to the CRM Worksheet. See the examples below:

- Customer responsibilities noted with "<ServiceName A>:" are added if <ServiceName A> is an optional service that can be used by the customer.
- Customer responsibilities noted with "<ServiceName B>:" are added if <ServiceName B> is an optional service that can be used by the customer.

• Example CRM responses, for sample Control IDs, are provided in the Example CRM Worksheet Responses sheet of this workbook.

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
AC-02	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-02 (01)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-02 (02)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-02 (03)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-02 (05)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-02 (07)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-02 (09)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-02 (10)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-02 (12)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-03	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8
AC-08	Partial	Federal customers are responsible for implementing a screen lock for their users. New Relic federal customers must federate their organizational Active Directory Service with the New Relic Observability Platform in order to achieve full compliance with FedRAMP session restriction requirements. For more information on federal customer user authentication, refer to IA-8.
AC-11	Partial	Federal customers are responsible for implementing a screen lock for their users. New Relic federal customers must federate their organizational Active Directory Service with the New Relic Observability Platform in order to achieve full compliance with FedRAMP session restriction requirements. For more information on federal customer user authentication, refer to IA-8.
AC-11(01)	Partial	Federal customers are responsible for implementing a screen lock for their users. New Relic federal customers must federate their organizational Active Directory Service with the New Relic Observability Platform in order to achieve full compliance with FedRAMP session restriction requirements. For more information on federal customer user authentication, refer to IA-8.
IA-02 (12)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8.
IA-04	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8.

IA-04 (04)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8.
IA-05	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8.
IA-05 (01)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8.
IA-05 (02)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8.
IA-05 (04)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8.
IA-05 (06)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8.
IA-05 (11)	Partial	The New Relic Observability Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic Observability Platform. New Relic Observability Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic Observability Platform web interface. New Relic federal customers must implement SSO functionality in order to comply with FedRAMP requirements. For more information on federal customer user authentication, refer to IA-8.
IR-09	Partial	New Relic Observability Platform is classified as a FIPS-199 moderate risk impact system, so classified data is not stored, processed, or transmitted within the system. It is the responsibility of federal customers to ensure that unauthorized information is not stored or transmitted within the New Relic Observability Platform.
IR-09(01)	Partial	New Relic Observability Platform is classified as a FIPS-199 moderate risk impact system, so classified data is not stored, processed, or transmitted within the system. It is the responsibility of federal customers to ensure that unauthorized information is not stored or transmitted within the New Relic Observability Platform.
IR-09(02)	Partial	New Relic Observability Platform is classified as a FIPS-199 moderate risk impact system, so classified data is not stored, processed, or transmitted within the system. It is the responsibility of federal customers to ensure that unauthorized information is not stored or transmitted within the New Relic Observability Platform.
IR-09(03)	Partial	New Relic Observability Platform is classified as a FIPS-199 moderate risk impact system, so classified data is not stored, processed, or transmitted within the system. It is the responsibility of federal customers to ensure that unauthorized information is not stored or transmitted within the New Relic Observability Platform.
IR-09(04)	Partial	New Relic Observability Platform is classified as a FIPS-199 moderate risk impact system, so classified data is not stored, processed, or transmitted within the system. It is the responsibility of federal customers to ensure that unauthorized information is not stored or transmitted within the New Relic Observability Platform.
RA-2	Partial	Federal customers must separately categorize their data in agreement with FIPS 199 and NIST 800-60 to ensure that the security category of information types collected, processed, or supported by the New Relic Observability Platform do not exceed FIPS 199 Moderate impact for confidentiality, integrity, and/or availability.
SA-04(10)	Partial	New Relic uses SAML SSO to provide federal customers the ability to establish a trust relationship with their onsite account management systems with the New Relic SAML SSO. Once a trust relationship is established between a federal customer's account management system and the New Relic SAML SSO, federal customers will be able to integrate their existing identification and authentication actions with the New Relic Observability Platform environment. The SAML-based SSO will allow customers to leverage existing internal PIV capabilities and FICAM third-party credentials. In order to comply with FedRAMP requirements, New Relic customers must federate their account management tool with the New Relic SAML SSO.
SC-7	Partial	Federal Customers are responsible for updating their configuration to point to the new FedRAMP authorized endpoints dedicated for FedRAMP sensitive customers. This configuration update will ensure that their data does not pass through non-FedRAMP authorized CDN. FedRAMP Compliant Endpoints Refer to SC-7 and SC-8 for more information.
SC-8	Partial	Federal Customers are responsible for updating their configuration to point to the new FedRAMP authorized endpoints dedicated for FedRAMP sensitive customers. This configuration update will ensure that their data does not pass through non-FedRAMP authorized CDN. FedRAMP Compliant Endpoints Refer to SC-7 and SC-8 for more information.
SC-08(01)	Partial	Federal customers are responsible to install the New Relic agents based on their applications coding language. Various agents include PHP, C, Go, Java, .Net, Python, Node.js, and Ruby. The agents implement cryptographic mechanisms to prevent the unauthorized disclosure of information during transmission through library dependencies and code development. Customers are responsible for certification and accreditation of these components as part of the on premise FISMA authorization efforts for continuous monitoring which includes activities such as updating and patching of these components in coordination with New Relic. Customers are responsible to meet the applicable System and Information Integrity (SI) controls associated with these components. For additional information, refer to SC-8(1).
SC-17	Partial	Customers are responsible for configuring their web browsers and workstations to prohibit unencrypted communications and ensuring they have implemented the appropriate trusted Certificate Authorities. Refer to IA-8 for more information on federal customer account management, access enforcement, and authentication.
SC-20	Partial	Enforcement of TLS 1.2 is dependent on customer's infrastructure capability. By default TLS 1.2 is used unless specified in the SLA or contract agreement by customer request. If TLS 1.2 is not used, customer assumes responsibilities on their data across the NROne boundary.
SC-21	Partial	Enforcement of TLS 1.2 is dependent on customer's infrastructure capability. By default TLS 1.2 is used unless specified in the SLA or contract agreement by customer request. If TLS 1.2 is not used, customer assumes responsibilities on their data across the NROne boundary.
SC-23	Partial	Federal Customers are responsible for configuring their web browsers and workstations to prohibit unencrypted communications and ensuring they have implemented the appropriate trusted Certificate Authorities. Refer to IA-8 for more information on federal customer account management, access enforcement, and authentication.