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:

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
AC-02	Partial	The New Relic One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One 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 One 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 One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One Platform uses SAML SSO to provide federal customers the ability to leverage their internal account management and authentication infrastructure with the New Relic One Platform. New Relic One Platform SSO functionality allows federal customers to use their own PIV authenticators and FICAM third-party credentials to authenticate to the New Relic One 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 One 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 One Platform.
IR-09(01)	Partial	New Relic One 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 One Platform.
IR-09(02)	Partial	New Relic One 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 One Platform.
IR-09(03)	Partial	New Relic One 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 One Platform.
IR-09(04)	Partial	New Relic One 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 One 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 One 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 One 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.