New Relic Observability Platform
FedRAMP Moderate Customer Responsibility Matrix (CRM) Worksheet

This CRM provides details for a Customer of what their responsibilities are for a given control, including responsibilities for optional services (applicable depending on which services the customer acquires). The CRM contains information for what a Customer needs to implement in order to obtain and maintain their authorization/certification. The Customer responsibility outlines the remaining controls that need to be implemented by the leveraging entity for compliance.

GUIDANCE:

1. Review the CRM to define all the controls that will need to be engineered, designed, defined and implemented in order to be in compliance with the FedRAMP baseline.
2. Mark controls with "Yes" designation in the "Can Be Inherited from CSP" column as Fully Inherited from New Relic F1607057910 FedRAMP Authorized: 03/02/2020.
3. Mark controls with "Partial" designation in the "Can Be Inherited from CSP" column as Partially Inherited from New Relic F1607057910 FedRAMP Authorized: 03/02/2020. Customers must describe their responsibilities in their Customer-level system security plan.
4. Controls with a "No" designation in the "Can Be Inherited from CSP" column cannot be Fully nor Partially inherited. Customers must describe their responsibilities in their Customer-level system security plan.

Control ID	Can Be Inherited from CSP	Specific Inheritance and Customer Agency/CSP Responsibilities
AC-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
AC-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
AC-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customers policy and procedure management lifecycle.
AC-2(a)	Yes	
AC-2(b)	No	Customers must assign account managers for its users.
AC-2(c)	No	Customers should establish conditions for group and role membership in accordance with their access control requirements.
AC-2(d)	No	Customers should identify users within their organization and specify the conditions for those users to belong to groups and be assigned platform roles. This can be achieved by establishing a New Relic account structure. See Introduction to user management and Important user management concepts.

AC-2(e)	No	Customers should require approval for each platform account type requested in accordance with their access control requirements.
AC-2(f)	No	Customers should perform all account management activities (e.g., creation, enablement, modification, disablement, and removal) in accordance with their access control requirements. Customers can utilize New Relic's SAML SSO and SCIM provisioning features to set up automatic controls. See Get started with SAML SSO and/or SCIM.
AC-2(g)	Partial	Customers should monitor use of their platform end user accounts. Customers can use NrAuditEvent and set up alerts to meet their monitoring needs. See NRAuditEvent: Query account audit logs.
AC-2(h)	No	Customers should notify its account managers when accounts are no longer needed and personnel with accounts and platform access are terminated or transferred or when their usage or need-to-know changes in accordance with their access control requirements.
AC-2(i)	No	Customers should only grant access to the platform based on their established access control requirements. See Important user management concepts.
AC-2(j)	No	Customers should review their platform end user accounts for compliance with their established account management requirements at a frequency and in accordance with their access control requirements.
AC-2(k)	No	If Customers share credentials, they should establish a process for changing credentials in the event that a person's access is removed or terminated.
AC-2(l)	No	Customers should ensure that they align their platform account management processes with their personnel termination and transfer process to ensure former personnel do not retain access to resources.
AC-2(1)	Partial	Customers can enable automated user management (AUM). Customers can import, update, and deactivate New Relic platform users via SCIM provisioning from their identity provider (for example, Azure AD, Okta, or OneLogin).
AC-2(2)	No	Should Customers utilize temporary and/or emergency accounts, Customers can provision these account types within their identity and access management infrastructure to comply with FedRAMP requirements. New Relic's SAML SSO and SCIM provisioning features that allows its Customer end users to use their own PIV authenticators andFICAM third-party credentials to identify and authenticate onto the platform, enabling Customers to meet their identity and access management compliance needs (e.g., PIV SSO, etc.). See Get started with SAML SSO and/or SCIM. Otherwise, Customers will need to monitor their platform to remove temporary and/or emergency accounts to satisfy this requirement.
AC-2(3)(a)	No	Customers should ensure that they disable or delete any of their end user accounts that are no longer needed.
AC-2(3)(b)	No	Customers should ensure that they disable or delete any of their end user accounts that are no longer needed.
AC-2(3)(c)	No	Customers should ensure that they disable or delete any of their end user accounts that have violated policy.
AC-2(3)(d)	No	If a Customer is using New Relic's SAML SSO and SCIM provisioning features then they should ensure that their identity infrastructure is configured to disable their user's accounts if they have been inactive for 90 days.
AC-2(4)	Partial	In addition to using NRAuditEvent to query account management events, Customers can enable audit configuration settings within their identity and access management infrastructure to capture additional account management activities. New Relic's SAML SSO and SCIM provisioning features that allows its Customer end users to use their own PIV authenticators and FICAM third-party credentials to identify and authenticate onto the platform, enabling Customers to meet their identity and access management compliance needs (e.g., PIV SSO, etc.).
AC-2(5)	No	Customers are subjected to New Relic's Rules of Behavior and are responsible for enforcing its requirements, such as requiring platform users to log out at the end of their standard word period.
AC-2(7)(a)	No	Customers should establish privileged user access in accordance with their access control requirements. See User type: basic, core, and full platform users and Important user management concepts.
AC-2(7)(b)	No	Customers should monitor their user account privileges in accordance with their access control requirements.

AC-2(7)(c)	Partial	If a Customer creates custom roles, then they should monitor changes to those customer roles. See Create custom roles (optional).
AC-2(7)(d)	No	Customers should revoke or remove access to privileged roles when they are no longer appropriate.
AC-2(9)	No	Customers can share an account if they so choose and should only do so in accordance with their access control requirements.
AC-2(12)(a)	No	Customers should monitor their end user accounts for atypical usage.
AC-2(12)(b)	No	Customers should monitor their end user accounts for atypical usage.
AC-2(13)	No	Customers should disable the accounts of any of their users who pose a significant security and/or privacy risk.
AC-3	Partial	If a Customer has enabled SAML, they must create groups to ensure that their users have access to accounts or roles. See Important user management concepts.
AC-4	Yes	
AC-4(21)	Yes	
AC-5(a)	No	Customers should separate duties of its users when prescribing roles to ensure access granted is not overly permissive.
AC-5(b)	Yes	
AC-6	No	Customers should administer platform end user accounts and access to satisfy least privilege principles. New Relic provides roles based access control features, see Introduction to use management.
AC-6(1)(a)	No	Customers must assign roles and permissions to govern access to security functions and security relevant information. See User permissions.
AC-6(1)(b)	No	Customers must assign roles and permissions to govern access to security functions and security relevant information. See User permissions.
AC-6(2)	No	Customers are responsible for ensuring that their users adhere to New Relic's FedRAMP Rules of Behavior.
AC-6(5)	No	Customers should only establish privileged accounts or privileged access for specific personnel or teams. See Introduction to user management.
AC-6(7)(a)	No	If customers create custom roles, they should ensure that they review those custom roles at least annually to validate the need. See User permissions.
AC-6(7)(b)	No	If a Customer determines that a custom role and/or its permissions are no longer needed, they should remove or modify. See User permissions.
AC-6(9)	Yes	
AC-6(10)	Yes	
AC-7(a)	Partial	Customers should ensure that their identity infrastructure is configured to satisfy this control if they utilize New Relic's SAML SSO and SCIM provisioning features that allows its Customer end users to use their own PIV authenticators andFICAM third-party credentials to identify and authenticate onto the platform.
AC-7(b)	No	Customers should follow the appropriate Password-related troubleshooting guidance to reset passwords to regain access to the platform.
AC-8(a)		Customers can ensure that their users are required to access the system from Customer-issued devices that have system use notification on the mobile device login page in order to satisfy this control since this is not in place at the New Relic Observability Platform's system-level.

AC-8(b)		Customers can ensure that their users are required to access the system from Customer-issued devices that have system use notification on the mobile device login page in order to satisfy this control since this is not in place at the New Relic Observability Platform's system-level. A customer's mobile device will retain the system warning banner until the user explicitly identifies and authenticates onto the device.
AC-8(c)	Yes	
AC-11(a)	No	Customers should configure device locks in accordance with their mobile device management policies and procedures to satisfy this requirement.
AC-11(b)	No	Customers should configure device locks in accordance with their mobile device management policies and procedures to satisfy this requirement.
AC-11(1)	No	Customers should configure device locks in accordance with their mobile device management policies and procedures to satisfy this requirement.
AC-12	Partial	Customers can configure the length of time that users can remain logged in. See Other user-related settings.
AC-14(a)	Yes	
AC-14(b)	Yes	
AC-17(a)	Yes	
AC-17(b)	Yes	
AC-17(1)	Yes	
AC-17(2)	Partial	Customers can prohibit access over the internet and require its end users to be on their virtual private network prior to accessing the platform using SAML SSO. See Get started with SAML SSO and/or SCIM.
AC-17(3)	Yes	
AC-17(4)(a)	Yes	
AC-17(4)(b)	Yes	
AC-18(a)	No	Customers should establish wireless access requirements for their users who are authorized to access the platform over WiFi connections while on-premises or working from other locations.
AC-18(b)	No	If Customers mandate use of a virtual private network when accessing cloud services then they should leverage their organization's wireless infrastructure and protections for their users. This can be achieved through their access control practices (e.g. SAML and SCIM SSO configurations described in AC-2(f)), and VPN requirements may be inherited from their Common Control Program.
AC-18(1)	No	Customers can protect its wireless access over Wifi connections by requiring all of their users to use the organization's virtual private network and single sign on when accessing the platform. See Get started with SAML SSO and/or SCIM.
AC-18(3)	Yes	
AC-19(a)	No	Customers should establish access control requirements for mobile devices for their users who are authorized to access the platform using mobile devices such as smartphones or tablets.
AC-19(b)	No	Customers should explicitly authorize use of mobile devices for their users that access the platform.

AC-19(5)	No	Customer's should employ full-device encryption or container-based encryption to protect the confidentiality and integrity of information on their user mobile devices.
AC-20(a)	Yes	
AC-20(b)	Yes	
AC-20(1)(a)	Yes	
AC-20(1)(b)	Yes	
AC-20(2)	Yes	
AC-21(a)	Yes	
AC-21(b)	Yes	
AC-22(a)	Yes	
AC-22(b)	Yes	
AC-22(c)	Yes	
AC-22(d)	Yes	
AT-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
AT-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
AT-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customers policy and procedure management lifecycle.
AT-2(a)	No	Customers should ensure that they provide security and privacy literacy training to their workforce in accordance with their awareness and training program process and procedures.
AT-2(b)	No	Customers should ensure that they employ techniques to increase the security and privacy awareness across their organization in accordance with their awareness and training program process and procedures.
AT-2(c)	No	Customers should ensure that they review and update their security and privacy literacy training content in accordance with their awareness and training program process and procedures.
AT-2(d)	No	Customers should ensure that they incorporate lessons learned from security incidents or breaches into their security and privacy literacy training content during their review and update cycles in accordance with their awareness and training program process and procedures.
AT-2(2)	No	Customers should ensure that they include an insider threat module in the security and privacy literacy training provided to their workforce.
AT-2(3)	No	Customers should ensure that they include a social engineering and social mining module in the security and privacy literacy training provided to their workforce.
AT-3(a)	No	Customers should ensure that they provide role-based security and privacy training to their workforce in accordance with their awareness and training program process and procedures. New Relic also provides training at New Relic University.
AT-3(b)	No	Customers should ensure that they review and update their role-based security and privacy training content in accordance with their awareness and training program process and procedures.
AT-3(c)	No	Customers should ensure that they incorporate lessons learned from security incidents or breaches into their role-based security and privacy literacy training content during their review and update cycles in accordance with their awareness and training program process and procedures.

AT-4(a)	No	Customers should document and monitor their workforce's security and privacy training activities using their learning management system or other techniques in accordance with their awareness and training program process and procedures.
AT-4(b)	No	Customers should retain their workforce's security and privacy training records using their learning management system or other techniques in accordance with their awareness and training program process and procedures.
AU-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
AU-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
AU-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
AU-2(a)	Yes	
AU-2(b)	Yes	
AU-2(c)	Yes	
AU-2(d)	Yes	
AU-2(e)	Yes	
AU-3(a)	Yes	
AU-3(b)	Yes	
AU-3(c)	Yes	
AU-3(d)	Yes	
AU-3(e)	Yes	
AU-3(f)	Yes	
AU-3(1)	Yes	
AU-4	Yes	
AU-5(a)	Yes	
AU-5(b)	Yes	
AU-6(a)	No	Customers can monitor their accounts and review logs using NrAuditEvent: Query account audit logs.
AU-6(b)	No	Customers should report findings in accordance with their incident management process or other reporting requirements.
AU-6(c)	Yes	
AU-6(1)	Yes	
AU-6(3)	Yes	
AU-7(a)	Yes	
AU-7(b)	Yes	
AU-7(1)	Yes	
AU-8(a)	Yes	
AU-8(b)	Yes	
AU-9(a)	Yes	
AU-9(b)	Yes	
AU-9(4)	Yes	
AU-11	Partial	Customers can use New Relic's Live Archive feature to set a custom log record retention policy to meet their organization retention requirements.

AU-12(a)	Yes	
AU-12(b)	Yes	
AU-12(c)	Yes	
CA-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
CA-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
CA-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
CA-2(a)	Partial	Customers should select the appropriate assessor or assessment team to conduct an audit and assessment of its Customer-assigned/responsible controls in accordance with their assessment, authorization, and monitoring requirements.
CA-2(b)	Partial	Customers should work with their assessors or assessment team to develop a SAP that meets all parts of this requirement when preparing to assess the Customer-responsible controls.
CA-2(c)	Partial	Customers should ensure that their Authorizing Official or designee, approve of their internal SAP as well as New Relic's FedRAMP audit SAP.
CA-2(d)	Partial	Customers should assess the Customer-assigned security and privacy controls at least annually.
CA-2(e)	Partial	Customers should produce an audit and assessment report for the Customer-assigned security and privacy controls that they've implemented.
CA-2(f)	Partial	Customers should provide their SAR and New Relic's SAR to their AO.
CA-2(1)	No	Customers should employ independent assessors to assess Customer-assigned controls.
CA-2(3)	Partial	Customers should leverage New Relic-provided security assessment results when considering issuing an authorization decision if they believe that New Relic's audit has satisfied its organization's business and mission needs.
CA-3(a)	Partial	Customers must approve of New Relic's terms of service, which includes language about information/data exchange, when signing acquisition documentation.
CA-3(b)	Yes	
CA-3(c)	Yes	
CA-5(a)	No	Customers should develop POA&Ms for vulnerabilities related to their use of and implementation of Customer-assigned controls on this platform to satisfy this control.
CA-5(b)	No	Customers should update any POA&Ms related to their use of and implementation of Customer-assigned controls on this platform at least monthly to satisfy this control.
CA-6(a)	No	Customer are responsible for assigning a senior official to serve as their AO that will make the formal managerial decision to authorize Agency use of the New Relic Observability Platform.
CA-6(b)	No	Customer are responsible for assigning a senior official to serve as an AO that is responsible for the organization's common control program and that will make the formal managerial decision to make these controls available for inheritance.
CA-6(c)	No	Customer are responsible for ensuring that their AO (1) accepts the use of inherited common controls that would be in scope for their use of the New Relic Observability Platform (i.e., Customer Agencies must identify which controls that they can leverage from their common control program during their control tailoring exercise) and (2) issue an authorization to operate (ATO) decision at the Agency-level prior to use of the New Relic Observability Platform (i.e., OMB Circular A-130 requires Agencies to individually authorize operation of an information system and to explicitly accept the risk.).
CA-6(d)	No	Customer are responsible for ensuring that the AO of the Agency common control program has made a formal managerial decision to make available and inheritable common controls for New Relic Observability Platform Customer-responsible/assigned security and privacy controls. Please refer to the control implementation summary (CIS) workbook for more information.

CA-6(e)	No	Customers should update their org-level authorization of the platform in accordance with OMB A-130 requirements or when a significant change affects the existing authorization decision.
CA-7(a)	No	Customers should establish system-level monitoring metrics.
CA-7(b)	No	Customers should establish monitoring frequencies and perform annual assessments of the Customer-assigned security and privacy controls.
CA-7(c)	No	Customers should perform ongoing control assessments in accordance with their continuous monitoring strategy to satisfy this control.
CA-7(d)	Partial	Customers should monitor their use of the platform in accordance with their continuous monitoring strategy to satisfy this control. They should also participate in New Relic's Multi-Agency Continuous Monitoring cohort to monitor New Relic's platform security posture.
CA-7(e)	Partial	Customers should correlate and analyze continuous monitoring information and assessment results. This should also include New Relic monthly continuous monitoring information and annual assessment results.
CA-7(f)	No	Customers should establish response actions to address the results of the analysis of control assessment results and continuous monitoring information.
CA-7(g)	No	Customers should report the security and privacy status of their use of the platform and New Relic's continuous monitoring results to their Authorizing Official in accordance with their continuous monitoring strategy.
CA-7(1)	No	Customers should employ independent assessors or assessment teams to monitor the Customer-assigned controls that they are responsible for implementing to satisfy this control.
CA-7(4)(a)	No	Customers should ensure that risk monitoring is an integral part of the continuous monitoring strategy that includes effective monitoring.
CA-7(4)(b)	No	Customers should ensure that risk monitoring is an integral part of the continuous monitoring strategy that includes compliance monitoring.
CA-7(4)(c)	No	Customers should ensure that risk monitoring is an integral part of the continuous monitoring strategy that includes change monitoring.
CA-8	Yes	
CA-8(1)	Yes	
CA-8(2)	Yes	
CA-9(a)	Yes	
CA-9(b)	Yes	
CA-9(c)	Yes	
CA-9(d)	Yes	
CM-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
CM-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
CM-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
CM-2(a)	Yes	
CM-2(b)	Yes	
CM-2(2)	Yes	
CM-2(3)	Yes	
CM-2(7)(a)	Yes	
CM-2(7)(b)	Yes	

CM-3(a)	Yes	
CM-3(b)	Partial	Customer designated representatives participate in the review of significant change requests for components within or that impact the FedRAMP authorization boundary and voting Authorizing Officials must provide an approval/authorization decision in accordance with the New Relic Continuous Monitoring Charter. Significant changes are defined in the New Relic Continuous Monitoring Charter.
CM-3(c)	Yes	
CM-3(d)	Yes	
CM-3(e)	Yes	
CM-3(f)	Yes	
CM-3(g)	Yes	
CM-3(2)	Yes	
CM-3(4)	Yes	
CM-4	Partial	Customer should perform an impact analysis for New Relic presented significant changes prior to issue an approval or non-approval decision.
CM-4(2)	Yes	
CM-5	No	Customers should configure logical access restrictions to access to initiate changes to the system. Customers can use roles and permissions. See User permissions.
CM-5(1)(a)	Yes	
CM-5(1)(b)	Yes	
CM-5(5)(a)	Yes	
CM-5(5)(b)	Yes	
CM-6(a)	Partial	Customers should ensure that they configure New Relic Observability Platform features and capabilities to reflect the most secure configuration needed to meet their business and operational needs. See New Relic Docs and New Relic Developer.
CM-6(b)	Partial	Customers should implement their documented and approved configurations for the platform in accordance with their configuration and change management process and procedures.
CM-6(c)	Partial	Customers should identify, document, and approve of any deviations from their approved configuration baseline in accordance with their exception or deviation process.
CM-6(d)	Partial	Customers should monitor and control changes to their platform settings in accordance with their continuous monitoring and configuration and change management process and procedures. Customers can review all platform activities using the NrAuditEvent event to view audit logs that show changes in their New Relic organization, see NrAuditEvent: Query Account Audit Logs.
CM-6(1)	Yes	
CM-7(a)	No	Customers should configure the platform to only support their essential mission, function, and operational needs to satisfy their business requirements. See New Relic Docs and New Relic Developer.
CM-7(b)	Yes	
CM-7(1)(a)	Yes	
CM-7(1)(b)	Yes	
CM-7(2)	Yes	
CM-7(5)(a)	Yes	
CM-7(5)(b)	Yes	
CM-7(5)(c)	Yes	
CM-8(a)	Yes	
CM-8(b)	Yes	

CM-8(1)	Yes	
CM-8(3)(a)	Yes	
CM-8(3)(b)	Yes	
CM-9(a)	Yes	
CM-9(b)	Yes	
CM-9(c)	Yes	
CM-9(d)	Yes	
CM-9(e)	Yes	
CM-10(a)	Yes	
CM-10(b)	Yes	
CM-10(c)	Yes	
CM-11(a)	Yes	
CM-11(b)	Partial	Customers must adhere to prescribed agent compatibility and requirements. See Compatibility and requirements for New Relic agents and products.
CM-11(c)	Partial	Customers should monitor its end users actions within the platform, including installing software. Customers can query audit logs using NrAuditEvent, see more at NrAuditEvent: Query account audit logs.
CM-12(a)	Yes	
CM-12(b)	Yes	
CM-12(c)	Yes	
CM-12(1)	Yes	
CP-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
CP-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
CP-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
CP-2(a)	No	Customers should create a system-level ISCP for their use of the New Relic Observability Platform. Otherwise, Customers can choose to use an organization-level ISCP that may be inheritable from a Customer's common control program.
CP-2(b)	Partial	Customers should make readily available their ISCP and New Relic's FedRAMP ISCP to authorized personnel that have ISCP responsibilities.
CP-2(c)	No	Customers should coordinate their contingency planning activities with incident handling activities in accordance with their incident handling/management requirements. This may be inheritable from a Customer's common control program.
CP-2(d)	No	Customers should review their ISCP at least annually to satisfy this requirement. This may be inheritable from a Customer's common control program.
CP-2(e)	No	Customers should make necessary updates to their ISCP at the required frequency.. This may be inheritable from a Customer's common control program.
CP-2(f)	No	Customers should communicate changes about their contingency planning materials to relevant stakeholders to satisfy this requirement. This may be inheritable from a Customer's common control program.
CP-2(g)	No	Customers should incorporate lessons learned into their contingency planning activities and implement resulting changes
CP-2(h)	No	Customers should protect their contingency planning materials from unauthorized disclosure and modification. Customers should
CP-2(1)	No	Customers should coordinate system-level contingency planning development with the appropriate organization elements

CP-2(3)	Yes	
CP-2(8)	Yes	
CP-3(a)	No	Customers should provide contingency planning training to its platform uses in accordance with their contingency planning training
CP-3(b)	No	Customers should review and update their contingency planning training content in accordance with their incident response
CP-4(a)	No	Customers should test the effectiveness of their contingency planning capability using a scenario that best relates to their use of or
CP-4(b)	No	Customers should review contingency planning test results to satisfy this requirement.
CP-4(c)	No	Customers should initiate corrective actions, if needed, to satisfy this requirement.
CP-4(1)	No	Customers should coordinate contingency planning testing with other relevant plans (e.g., business continuity plans, disaster
CP-6(a)	Yes	
CP-6(b)	Yes	
CP-6(1)	Yes	
CP-6(3)	Yes	
CP-7(a)	Yes	
CP-7(b)	Yes	
CP-7(c)	Yes	
CP-7(1)	Yes	
CP-7(2)	Yes	
CP-7(3)	Yes	
CP-8	Yes	
CP-8(1)(a)	Yes	
CP-8(1)(b)	Yes	
CP-8(2)	Yes	
CP-9(a)	Yes	
CP-9(b)	Yes	
CP-9(c)	Yes	
CP-9(d)	Yes	
CP-9(1)	Yes	
CP-9(8)	Yes	
CP-10	Yes	
CP-10(2)	Yes	
IA-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
IA-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
IA-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
IA-2	Partial	Customers must create a unique username and password to identify and authenticate onto the platform to be provided access to its services and features. Customers can choose to use New Relic's SAML SSO and SCIM provisioning features that allows its Customer end users to use their own PIV authenticators and FICAM third-party credentials to identify and authenticate onto the platform. See Get started with SAML SSO and/or SCIM.

IA-2(1)	Partial	Customers can configure the platform to New Relic's SAML SSO and SCIM provisioning features that allows its Customer end users to use their own PIV authenticators andFICAM third-party credentials to identify and authenticate onto the platform. See Get started with SAML SSO and/or SCIM.
IA-2(2)	Partial	Customers can configure the platform to utilize New Relic's SAML SSO and SCIM provisioning features that allows its Customer end users to use their own PIV authenticators and FICAM third-party credentials to identify and authenticate onto the platform. See Get started with SAML SSO and/or SCIM.
IA-2(5)	Partial	In the event that Customers share accounts or authenticators, Customers should require users to be individually authenticated before granting access to the shared accounts or resources. See Get started with SAML SSO and/or SCIM.
IA-2(6)(a)	No	Customers can use New Relic's SAML SSO and/or SCIM features to satisfy MFA requirements. See Get started with SAML SSO and/or SCIM.
IA-2(6)(b)	No	Customers can use PIV or CAC cards as a part of their SAML SSO and/or SCIM integration.
IA-2(8)	Partial	Customers can use New Relic's SAML SSO and/or SCIM features to implement replay-resistant authentication mechanisms for access to the system. See Get started with SAML SSO and/or SCIM.
IA-2(12)	No	New Relic offers SAML SSO and SCIM provisioning features that allows its Customer end users to use their own PIV authenticators and FICAM third-party credentials to identify and authenticate onto the platform. This is further discussed under control IA-8 and its enhancements. See Get started with SAML SSO and/or SCIM.
IA-3	Yes	
IA-4(a)	No	Customers should obtain authorization to create platform user account identifiers.
IA-4(b)	No	Customers should select unique usernames for individual user accounts. Customers can also provision SAML SSO and/or SCIM. See Get started with SAML SSO and/or SCIM.
IA-4(c)	No	Customers should assign the username to the intended individual or group. Customers can also provision SAML SSO and/or SCIM. See Get started with SAML SSO and/or SCIM.
IA-4(d)	No	Customers should prevent reuse of usernames for at least two years. Customers can also provision SAML SSO and/or SCIM. See Get started with SAML SSO and/or SCIM.
IA-4(4)	Yes	
IA-5(a)	Yes	
IA-5(b)	Yes	
IA-5(c)	Partial	Customers can employ New Relic's SAML SSO and/or SCIM features to help enhance the security and protection of authenticators. See Get started with SAML SSO and/or SCIM.
IA-5(d)	Yes	
IA-5(e)	Yes	
IA-5(f)	Yes	
IA-5(g)	Yes	
IA-5(h)	Yes	
IA-5(i)	Yes	
IA-5(1)(a)	No	Customers should require their users to adhere to industry-wide practices when creating passwords.
IA-5(1)(b)	Yes	
IA-5(1)(c)	Yes	
IA-5(1)(d)	Yes	
IA-5(1)(e)	Yes	
IA-5(1)(f)	Partial	Customers should select passwords that satisfy New Relic password requirements as well as follow their organization's guidelines for password length, use of upper or lower case letters, numbers, and special characters.
IA-5(1)(g)	Yes	
IA-5(1)(h)	Yes	

IA-5(2)(a)	Partial	Customers can employ New Relic's SAML SSO and/or SCIM features tif they use public key-based authentication so that their users can log into their corporate idP using a PKI-based method. See Get started with SAML SSO and/or SCIM.
IA-5(2)(b)	Partial	If a Customers uses New Relic'sSAML SSO and/or SCIM feature, they must ensure that their identity and access management infrastructure validates certificates.
IA-5(6)	Yes	
IA-5(7)	Yes	
IA-6	Yes	
IA-7	Yes	
IA-8	Partial	Customers are responsible for enabling MFA capabilities for its non-privileged (or admin) users. New Relic offers SAML SSO and SCIM provisioning features that allows Customers to use their own PIV authenticators and FICAM third-party credentials to identify and authenticate. See Get started with SAML SSO and/or SCIM.
IA-8(1)	Partial	Customers are responsible for enabling and utilizing mutifactor authentication capabilities within their identity and access management infrastructure. New Relic Observability Platform offers SAML SSO and SCIM provisioning features that allows Customers to use their own PIV authenticators and FICAM third-party credentials to identify and authenticate, enabling Customers to meet their identity and access management compliance needs (e.g., PIV SSO, etc.).
IA-8(2)(a)	Partial	Customers can use New Relic's SAML SSO and/or SCIM features to satisfy external authenticator requirements. See Get started with SAML SSO and/or SCIM.
IA-8(2)(b)	Yes	
IA-8(4)	Partial	Customers can use New Relic's SAML SSO and/or SCIM features to satisfy identity management requirements. See Get started with SAML SSO and/or SCIM.
IA-11	No	The system will disconnect a Customer's session after the customer-configured period of inactivity, see Session-related setting. If a Customers has configured New Relic's SAML SSO and/or SCIM capabilities, they must ensure that they've applied the appropriate configuration settings to their identity and access management infrastructure that will enable them to comply with NIST SP 800-63 and FedRAMP requirements.
IA-12(a)	Partial	Customers should identity proof its workforce members that require access to the system.
IA-12(b)	Partial	Customers should resolve user accounts to a unique individual.
IA-12(c)	Partial	Customers should collect, validate, and verify provided identity proofing evidence for their workforce.
IA-12(2)	Partial	Customers should require evidence of individual identification be presented to the registration authority.
IA-12(3)	Partial	Customers should require that the presented identity evidence be validated and verified through its established methods of validation and verification.
IA-12(5)	Partial	Customers should use out-of-band methods to ensure that the individual associated with an address of record is the same individual that participated in the registration.
IR-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
IR-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
IR-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
IR-2(a)	Partial	Customers should provide incident response training to its platform uses in accordance with their incident response training requirements. This may be inheritable from a Customer's common control program.
IR-2(b)	Partial	Customers should review and update their incident response training content in accordance with their incident response training requirements. This may be inheritable from a Customer's common control program.
IR-3	Partial	Customers should test the effectiveness of their incident response capability using a use case that is related to their use of or that impacts their use of the New Relic Observability Platform. This may be inheritable from a Customer's common control program.

IR-3(2)	Partial	Customers should coordinate incident response testing with other relevant plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans, contingency plans, critical infrastructure plans, etc.).
IR-4(a)	Partial	Customers should implement an incident handling capacity that meets their incident handling/management requirements. This may be inheritable from a Customer's common control program.
IR-4(b)	Partial	Customers should coordinate their incident handling activities with contingency planning activities in accordance with their incident handling/management requirements. This may be inheritable from a Customer's common control program.
IR-4(c)	Partial	Customers should incorporate lessons learned into their incident management program and implement resulting changes accordingly.
IR-4(d)	Partial	Customers should ensure that their incident handling/management activities rigor, intensity, scope, and results are comparable and predictable enterprise wide.
IR-4(1)	Partial	Customers should employ automated mechanisms that support their incident handling process. Customers can incorporate the use of the Issues and incident management and response feature during their incident handling/management activities.
IR-5	Partial	Customers should track and maintain incident information and documentation. Customers can open an "incident" support case to track customer-impact incidents in the platform portal. Customers can also subscribe to New Relic's RSS feed to get security notification bulletins, more information at Security Bulletins.
IR-6(a)	Partial	Customers should require personnel to report suspected incidents to their incident response capability in accordance with their incident reporting requirements.
IR-6(b)	Partial	Customers must report suspected or confirmed incidents observed when using the platform to New Relic by notifying their account owners and opening a support case in the New Relic Observability Platform portal or by emailing security@newrelic.com or support@newrelic.com. Customers should also report suspected or confirmed incidents observed to their designated incident response personnel in accordance with their organization's incident response and management requirements.
IR-6(1)	Yes	
IR-6(3)	Yes	
IR-7	Partial	If a Customer suspects an incident or an confirmed security incident observed when using the platform, Customers should ensure that they provide users with an incident response support resource while handling and reporting the incident.
IR-7(1)	Yes	
IR-8(a)	Partial	Customers should create a system-level IRP or update their existing organization-wide IRP to capture, at a minimum, a communication and collaboration process with New Relic during an incident to inform their workforce.
IR-8(b)	Partial	Customers should distribute copies of their system-level IRP or updated organization-wide IRP to their workforce that use the New Relic Observability Platform.
IR-8(c)	Partial	Customers should update their system-level IRP or updated organization-wide IRP should there be any changes, including changes to their communication process with New Relic.
IR-8(d)	Partial	Customers should communicate updates to their system-level IRP or updated organization-wide IRP to their workforce with incident handling/response responsibilities, at a minimum.
IR-8(e)	Partial	Customers should protect their system-level IRP or updated organization-wide IRP from unauthorized disclosure and modification. Customers should also protect New Relic's FedRAMP IRP from unauthorized disclosure and modification if their workforce downloads copies.
IR-9(a)	Partial	Customers should assign a person with information spill response responsibilities to address information spill incidents.
IR-9(b)	Partial	The assigned Customer responding to the information spill incident should identify the specific information involved in the incident.
IR-9(c)	Partial	Customers should report suspected or known information spillage incidents related to or affecting the New Relic Observability Platform to their Incident Response Team and to New Relic using Zendesk. It is the full responsibility of the Customer to ensure that unauthorized information is not transmitted nor stored within the New Relic Observability Platform.
IR-9(d)	Partial	The assigned Customer responding to the information spill incident to take necessary measures to isolate contaminated components of the environment.
IR-9(e)	Partial	The assigned Customer responding to the information spill should work with New Relic to ensure that all unauthorized information is purged from the system environment/infrastructure.

IR-9(f)	Yes	
IR-9(g)	Partial	The assigned Customer should complete an after action report or take additional actions as defined by their incident response/management requirements.
IR-9(2)	No	Customers should provide information response/management training that includes an information spillage module.
IR-9(3)	Yes	
IR-9(4)	Partial	Customers should respond to unauthorized information access in accordance with their incident response/management requirements. In addition to reporting the information spill to New Relic, Customers should collaborate closely with New Relic to identify other potentially affected components and scope of the spill.
MA-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
MA-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
MA-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
MA-2(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-2(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-2(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-2(d)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-2(e)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-2(f)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-3(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-3(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-3(1)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-3(2)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.

MA-3(3)(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-3(3)(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-3(3)(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-3(3)(d)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-4(a)	Yes	
MA-4(b)	Yes	
MA-4(c)	Yes	
MA-4(d)	Yes	
MA-4(e)	Yes	
MA-5(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-5(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-5(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-5(1)(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-5(1)(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MA-6	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
MP-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
MP-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer’s policy and procedure management lifecycle.
MP-2	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.

MP-3(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-3(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-4(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-4(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-5(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-5(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-5(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-5(d)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-6(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-6(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-7(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
MP-7(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
PE-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
PE-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer’s policy and procedure management lifecycle.
PE-2(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.

PE-2(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-2(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-2(d)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-3(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-3(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-3(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-3(d)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-3(e)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-3(f)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-3(g)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-4	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-5	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-6(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-6(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-6(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.

PE-6(1)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-8(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-8(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-8(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-9	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-10(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-10(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-10(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-11	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-12	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-13	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-13(1)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-13(2)(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-13(2)(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-14(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.

PE-14(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-15	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-16(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-16(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-17(a)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-17(b)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-17(c)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PE-17(d)	No	The New Relic Observability Platform is a SaaS product fully deployed on top of AWS US East/West. New Relic fully inherits the implemented security and privacy protection mechanisms from AWS for this control requirement. Accordingly, this control is fully inheritable from AWS US East/West.
PL-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
PL-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
PL-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer’s policy and procedure management lifecycle.
PL-2(a)	Partial	Customers should created a system-level SSP to capture Customer-assigned control implementation details.
PL-2(b)	Partial	Customers should distribute or make readily available their system-level SSP to authorized personnel. Customers should distribute or make readily available the New Relic SSP in accordance with the FedRAMP Package Request requirements.
PL-2(c)	Partial	Customers should review their system-level SSP at least annually. Customers should also review New Relic’s SSP annually for any updates and changes.
PL-2(d)	Partial	Customers should update their system-level SSP as needed.
PL-2(e)	Partial	Customers should protect their system-level SSP from unauthorized modification and disclosure. Customers should protect New Relic’s SSp from unauthorized modification and disclosure in accordance with the FedRAMP Package Request requirements.
PL-4(a)	Partial	Customers are responsible for ensuring that their users receive a copy of New Relic provided FedRAMP ROB.
PL-4(b)	Partial	Customers should ensure that they receive a signed acknowledgement from their users.
PL-4(c)	Yes	
PL-4(d)	Partial	Customers must ensure that their users read and re-acknowledge the New Relic-provided FedRAMP ROB at least annually and when the rules are revised or changed to satisfy this control.
PL-4(1)(a)	Yes	
PL-4(1)(b)	Yes	

PL-4(1)(c)	Yes	
PL-8(a)	Yes	
PL-8(b)	Yes	
PL-8(c)	Yes	
PL-10	Partial	Customers should refer to the New Relic provided Customer Implementation Summary workbook to select and apply the Customer assigned security and privacy controls to their implementation of the New Relic Observability Platform. The FedRAMP control baseline is slightly different from the FISMA control baseline, and this will help ensure that Customers reflect both requirements adequately.
PL-11	Partial	Customers should tailor Customer-assigned controls leveraging NIST 800-53B (e.g., apply scoping parameters, specify and assign Customer-defined parameters, etc.).
PS-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
PS-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
PS-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
PS-2(a)	No	Customers should assign a risk designation to all of its organization positions in accordance with their personnel security requirements. This may be inheritable from a Customer's common control program.
PS-2(b)	No	Customers should establish screening criteria in accordance with their personnel security requirements. This may be inheritable from a Customer's common control program.
PS-2(c)	No	Customers should review and update position risk designations at least every three years to comply with FedRAMP-defined requirements. This may be inheritable from a Customer's common control program.
PS-3(a)	No	Customers should screen individuals prior to granting them access to the New Relic Observability Platform. This may be inheritable from a Customer's common control program.
PS-3(b)	No	Customers should rescreen its personnel in accordance with their personnel security requirements. This may be inheritable from a Customer's common control program.
PS-3(3)(a)	No	Customers should verify the access authorizations of personnel that will be accessing the New Relic Observability Platform in accordance with their personnel security requirements.
PS-3(3)(b)	No	Customers should ensure that the persons that will be accessing the New Relic Observability platform satisfy any additional personnel screening criteria that they've defined. This may be inheritable from a Customer's common control program.
PS-4(a)	No	Customers should disable departing employees access to the New Relic Observability Platform.
PS-4(b)	No	Customers should terminate or revoke any authenticators associated with a departing employee's New Relic Observability Platform account. See Introduction to user management.
PS-4(c)	No	Customers should include security topics in exit interviews with employees that have had access to the New Relic Observability Platform. This may be inheritable from a Customer's common control program.
PS-4(d)	Yes	
PS-4(e)	Yes	
PS-5(a)	No	Customers should review and confirm ongoing operational need for current logical access authorization to the New Relic Observability Platform when individuals are reassigned or transferred to other positions within their organization.
PS-5(b)	No	Customers should initiate transfer or reassignment actions within 24 hours of a formal transfer decision. This may be inheritable from a Customer's common control program.
PS-5(c)	No	Customers should modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer. See User permissions.

PS-5(d)	No	Customers should notify necessary stakeholders within 24 hours of a formal transfer decision. This may be inheritable from a Customer’s common control program.
PS-6(a)	Yes	
PS-6(b)	Yes	
PS-6(c)	No	Customers should ensure that their system end users sign and resign at least annually and any time there is a change to the user's level of access the New Relic Observability FedRAMP Rules of Behavior.
PS-7(a)	Yes	
PS-7(b)	Yes	
PS-7(c)	Yes	
PS-7(d)	Yes	
PS-7(e)	Yes	
PS-8(a)	No	Customers should employ a formal sanctions process for individuals failing to comply with established information security and privacy procedures. This may be inheritable from a Customer’s common control program. This may be inheritable from a Customer’s common control program.
PS-8(b)	No	Customers should notify appropriate stakeholders within 24 hours of a formal employee sanctions process being initiated. This may be inheritable from a Customer’s common control program.
PS-9	Yes	
RA-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
RA-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
RA-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer’s policy and procedure management lifecycle.
RA-2(a)	No	Customers must separately categorize the data that they intend to transmit, store, and process with the New Relic Observability Platform to ensure compatibility with the overall criticality level of the platform.
RA-2(b)	No	Customers should document the results of their FIPS 199 security categorization results of their data in their Customer-level SSP.
RA-2(c)	No	Customers must ensure that their assigned AO reviews and approves of the FIPS 199 security categorization results of their data.
RA-3(a)	Yes	
RA-3(b)	Yes	
RA-3(c)	Yes	
RA-3(d)	Partial	Customers should review New Relic’s FedRAMP security assessment results on at least an annual basis.
RA-3(e)	Yes	
RA-3(f)	Yes	
RA-3(1)(a)	Yes	
RA-3(1)(b)	Yes	
RA-5(a)	Yes	
RA-5(b)	Yes	
RA-5(c)	Yes	
RA-5(d)	Yes	
RA-5(e)	Yes	
RA-5(f)	Yes	
RA-5(2)	Yes	

RA-5(3)	Yes	
RA-5(5)	Yes	
RA-5(11)	Partial	Customers can use the system's portal to report cases of identified or suspected vulnerabilities and report issues for public open sourced agents in Github.
RA-7	Yes	
RA-9	Yes	
SA-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
SA-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
SA-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
SA-2(a)	Yes	
SA-2(b)	Yes	
SA-2(c)	Yes	
SA-3(a)	Yes	
SA-3(b)	Yes	
SA-3(c)	Yes	
SA-3(d)	Yes	
SA-4(a)	Yes	
SA-4(b)	Yes	
SA-4(c)	Yes	
SA-4(d)	Yes	
SA-4(e)	Yes	
SA-4(f)	Yes	
SA-4(g)	Yes	
SA-4(h)	Yes	
SA-4(i)	Yes	
SA-4(1)	Yes	
SA-4(2)	Yes	
SA-4(9)	Yes	
SA-4(10)	Partial	Customers are responsible for enabling and utilizing MFA capabilities within their identity and access management infrastructure. The system has SAML SSO and SCIM provisioning features that allows Customers to use their own PIV authenticators and FICAM third-party credentials to identify and authenticate, enabling Customers to meet their identity and access management compliance needs (e.g., PIV SSO, etc.). See Get started with SAML SSO and/or SCIM.
SA-5(a)	Yes	
SA-5(b)	Yes	
SA-5(c)	Yes	
SA-5(d)	Yes	
SA-8	Yes	
SA-9(a)	Yes	

SA-9(b)	Yes	
SA-9(c)	Yes	
SA-9(1)(a)	Yes	
SA-9(1)(b)	Yes	
SA-9(2)	Yes	
SA-9(5)	Yes	
SA-10(a)	Yes	
SA-10(b)	Yes	
SA-10(c)	Yes	
SA-10(d)	Yes	
SA-10(e)	Yes	
SA-11(a)	Yes	
SA-11(b)	Yes	
SA-11(c)	Yes	
SA-11(d)	Yes	
SA-11(e)	Yes	
SA-11(1)	Yes	
SA-11(2)(a)	Yes	
SA-11(2)(b)	Yes	
SA-11(2)(c)	Yes	
SA-11(2)(d)	Yes	
SA-15(a)	Yes	
SA-15(b)	Yes	
SA-15(3)(a)	Yes	
SA-15(3)(b)	Yes	
SA-22(a)	Yes	
SA-22(b)	Yes	
SC-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
SC-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
SC-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
SC-2	Yes	
SC-4	Yes	
SC-5(a)	Yes	
SC-5(b)	Yes	
SC-7(a)	Yes	
SC-7(b)	Yes	
SC-7(c)	Partial	Customers should adjust their configuration settings to send data with New Relic agents, integrations, and APIs to the relevant FedRAMP endpoint as described in FedRAMP compliant endpoints.
SC-7(3)	Yes	

SC-7(4)(a)	Yes	
SC-7(4)(b)	Yes	
SC-7(4)(c)	Yes	
SC-7(4)(d)	Yes	
SC-7(4)(e)	Yes	
SC-7(4)(f)	Yes	
SC-7(4)(g)	Yes	
SC-7(4)(h)	Yes	
SC-7(5)	Yes	
SC-7(7)	Yes	
SC-7(8)	Yes	
SC-7(12)	Yes	
SC-7(18)	Yes	
SC-8	Partial	Customers must ensure that they comply with requirements for using New Relic's FedRAMP environment, and then use New Relic FedRAMP-compliant endpoints to get data into the platform via agent configuration or API. New Relic has created dedicated "FedRAMP compliant endpoints" for Customer traffic. All traffic to and through these endpoints are encrypted using TLS1.2. The agents implement cryptographic mechanisms to prevent the unauthorized disclosure of information during transmission through library dependencies and code development. Please refer to section "Installation and Configuration" on https://docs.newrelic.com/ for more information.
SC-8(1)	Partial	Customers must ensure that they comply with requirements for using New Relic's FedRAMP environment, and then use New Relic FedRAMP-compliant endpoints to get data into the platform via agent configuration or API. All traffic to and through these endpoints are encrypted using TLS 1.2 or above. The agents implement cryptographic mechanisms to prevent the unauthorized disclosure of information during transmission through library dependencies and code development. Please refer to section "Installation and Configuration" on https://docs.newrelic.com/ for more information.
SC-10	Partial	Customers should ensure that their organization's corporate network or virtual private network is configured to terminate network connection after the required period of inactivity.
SC-12	Yes	
SC-13(a)	Yes	
SC-13(b)	Yes	
SC-15(a)	Yes	
SC-15(b)	Yes	
SC-17(a)	No	Customers are responsible for configuring their web browsers and workstations to prohibit unencrypted communications and ensuring they have implemented the appropriate trusted Certificate Authorities.
SC-17(b)	No	Customers are responsible for including only approved trust anchors in trust stores or certificate stores managed by their organization.
SC-18(a)	Yes	
SC-18(b)	Yes	
SC-20(a)	Yes	
SC-20(b)	Yes	
SC-21	Yes	
SC-22	Yes	

SC-23	No	Customers must upgrade to an operating system and/or TLS stack that supports TLS 1.2 or above. Customers accessing http://api.newrelic.com with clients not configured to follow redirects should ensure that their clients specify the https:// scheme (as opposed to http://), or that they are configured to follow redirects, such as by using the `-L` flag when using cURL.
SC-28	Yes	
SC-28(1)	Yes	
SC-39	Yes	
SC-45	Yes	
SC-45(1)(a)	Yes	
SC-45(1)(b)	Yes	
SI-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
SI-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
SI-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
SI-2(a)	Yes	
SI-2(b)	Yes	
SI-2(c)	Yes	
SI-2(d)	Yes	
SI-2(2)	Yes	
SI-2(3)(a)	Yes	
SI-2(3)(b)	Yes	
SI-3(a)	Yes	
SI-3(b)	Yes	
SI-3(c)	Yes	
SI-3(d)	Yes	
SI-4(a)	Yes	
SI-4(b)	Yes	
SI-4(c)	Yes	
SI-4(d)	Yes	
SI-4(e)	Yes	
SI-4(f)	Yes	
SI-4(g)	Yes	
SI-4(1)	Yes	
SI-4(2)	Yes	
SI-4(4)(a)	Yes	
SI-4(4)(b)	Yes	
SI-4(5)	Yes	
SI-4(16)	Yes	
SI-4(18)	Yes	
SI-4(23)	Yes	

SI-5(a)	Yes	
SI-5(b)	Yes	
SI-5(c)	Yes	
SI-5(d)	Yes	
SI-6(a)	Yes	
SI-6(b)	Yes	
SI-6(c)	Yes	
SI-6(d)	Yes	
SI-7(a)	Yes	
SI-7(b)	Yes	
SI-7(1)	Yes	
SI-7(7)	Yes	
SI-8(a)	Yes	
SI-8(b)	Yes	
SI-8(2)	Yes	
SI-10	Yes	
SI-11(a)	Yes	
SI-11(b)	Yes	
SI-12	Yes	
SI-16	Yes	
SR-1(a)	No	Customers should produce policies and procedures that satisfy FedRAMP-defined requirements for their workforce. New Relic does not govern nor have insight into its Customers policies and procedures.
SR-1(b)	No	Customers should designate personnel to manage the development, documentation, and dissemination of its policies and procedures.
SR-1(c)	No	Customers should perform reviews and updates to their policies and procedures such that they satisfy FedRAMP-defined requirements. New Relic does not govern nor have insight into its Customer's policy and procedure management lifecycle.
SR-2(a)	Yes	
SR-2(b)	Yes	
SR-2(c)	Yes	
SR-2(1)	Partial	If a Customers uses New Relic's SAML SSO and/or SCIM feature, they must ensure that their identity and access management infrastructure validates certificates.
SR-3(a)	Yes	
SR-3(b)	Yes	
SR-3(c)	Yes	
SR-5	Yes	
SR-6	Partial	Customers should assess and review supply chain-related risks associated with their use of the system at least annually to satisfy this control. This may be inheritable from a Customer's common control program.
SR-8	Partial	Customers should establish necessary agreements and procedures to satisfy this control. This may be inheritable from a Customer's common control program.
SR-10	Yes	
SR-11(a)	Yes	

SR-11(b)	Yes
SR-11(1)	Yes
SR-11(2)	Yes
SR-12	Yes