

Customer Responsibility Matrix

Coralogix US GovOps — FedRAMP Moderate

153 responsibilities

This matrix lists **only what your organization is responsible for** when using Coralogix US GovOps. The cards below give you the big picture in plain language; the sections underneath have the full detail, organized by task, with each item traceable to the specific FedRAMP control it covers. Controls that Coralogix fully manages, or that don't apply to a cloud-hosted SaaS platform with no customer-side physical infrastructure, aren't listed at all.

The big picture

Seven things, roughly. Click any card's controls below for the full detail.



Access & Identity 30

Managing who on your team can get in, and how — through your own identity provider.



Your Own Policies 20

Written policies covering your use of GovOps. If you already have broad security policies, this is usually just confirming they extend here.



People 11

Basic security hygiene for your personnel — training, screening, offboarding.



Keeping Your Own Systems Secure 37

Configuration, patching, monitoring, and encryption for anything you manage that connects to GovOps.



Monitoring & Assessment 22

Reviewing your own audit logs and periodically checking your own risk.



When Things Go Wrong 14

Knowing how to report a problem to us fast, and having your own recovery plan.



Vendors & Acquisition 19

Basic diligence if you build, buy, or use third-party systems that connect to GovOps.

JUMP TO A SECTION

[Policy Foundations — Required for Every Control Family](#)15[AC — Access Control](#)19[AT — Awareness and Training](#)3[AU — Audit and Accountability](#)10[CA — Assessment, Authorization, and Monitoring](#)6[CM — Configuration Management](#)12[CP — Contingency Planning](#)6[IA — Identification and Authentication](#)11[IR — Incident Response](#)8[PL — Planning](#)5[PS — Personnel Security](#)8[RA — Risk Assessment](#)6[SA — System and Services Acquisition](#)11[SC — System and Communications Protection](#)14[SI — System and Information Integrity](#)11[SR — Supply Chain Risk Management](#)8

Policy Foundations — Required for Every Control Family

Every control family below has one control asking whether your organization has a written policy for that area. Coralogix's own FedRAMP authorization covers how Coralogix operates its platform — it doesn't, and can't, cover how your organization manages your own people's access decisions, your own incident escalation, or your own personnel screening. These are governance questions specific to your organization that no vendor's certification can answer for you: who's accountable, how often the policy is reviewed, and how it's communicated internally. If your organization already has broader security policies covering these areas, the bar here is usually just confirming they extend to your use of GovOps — not building something from scratch. If you're a federal agency, contractor pursuing your own ATO, or otherwise subject to your own audit, your assessor will ask whether you have this documentation regardless of Coralogix's own authorization status.

Access Control (AC-1)

Develop, document, and keep current your own access control policy and procedures governing your use of Coralogix US GovOps, including any identity provider (IdP) configuration requirements.

Covers: AC-1(a), AC-1(b)

Awareness and Training (AT-1)

Develop and keep current your own security awareness and training policy covering your personnel's use of GovOps.

Covers: AT-1(a), AT-1(b), AT-1(c)

Audit and Accountability (AU-1)

Develop and keep current your own policy covering review of audit logs generated by your activity in GovOps. The policy should designate responsible officials and define the scope of audit activities for your personnel.

Covers: AU-1(a), AU-1(b), AU-1(c)

Assessment, Authorization, and Monitoring (CA-1)

Develop and keep current your own policy governing assessment of your systems that leverage GovOps.

Covers: CA-1(a), CA-1(b), CA-1(c)

Configuration Management (CM-1)

Develop and keep current your own policy covering configuration of your use of GovOps.

Covers: CM-1(a), CM-1(b), CM-1(c)

Contingency Planning (CP-1)

Develop and keep current your own policy for how your organization responds to a GovOps disruption.

Covers: CP-1(a), CP-1(b), CP-1(c)

Identification and Authentication (IA-1)

Develop and keep current your own policy covering your IdP configuration and authentication standards.

Covers: IA-1(a), IA-1(b), IA-1(c)

Incident Response (IR-1)

Develop and keep current your own policy, including how and when to notify Coralogix of a suspected incident.

Covers: IR-1(a), IR-1(b), IR-1(c)

Planning (PL-1)

Develop and keep current your own policy covering how your organization documents security plans that reference GovOps as an inherited authorization.

Covers: PL-1(a), PL-1(b), PL-1(c)

Personnel Security (PS-1)

Develop and keep current your own policy covering screening, access, and termination for personnel who access GovOps.

Covers: PS-1(a), PS-1(b), PS-1(c)

Risk Assessment (RA-1)

Develop and keep current your own policy covering risks introduced by your GovOps integration.

Covers: RA-1(a), RA-1(b), RA-1(c)

System and Services Acquisition (SA-1)

Develop and keep current your own policy for procuring systems and services that connect to GovOps.

Covers: SA-1(a), SA-1(b), SA-1(c)

System and Communications Protection (SC-1)

Develop and keep current your own policy covering protection of communications with GovOps.

Covers: SC-1(a), SC-1(b), SC-1(c)

System and Information Integrity (SI-1)

Develop and keep current your own policy governing the integrity of information processed through GovOps.

Covers: SI-1(a), SI-1(b), SI-1(c)

Supply Chain Risk Management (SR-1)

Develop and keep current your own policy covering the acquisition of systems and services connected to GovOps.

Covers: SR-1(a), SR-1(b), SR-1(c)

Manage user accounts through your identity provider

Manage accounts through your IdP, covering:

- Set up: define account types, assign an account manager, require approval before creating new accounts
- Specify access: define authorized users/groups/access per account, and authorize based on valid need
- Lifecycle: create, modify, disable, and remove accounts per your procedures, automating where possible
- Monitor & review: monitor account use, notify managers on termination/role changes, review periodically
- Shared accounts: restrict use to defined conditions; reissue credentials when someone leaves the group
- Auditability: ensure account actions are logged; monitor privileged accounts for atypical use and report it
- Roles: define role/permission assignments consistent with your access control policy

Covers: AC-2(a), AC-2(b), AC-2(c), AC-2(d), AC-2(e), AC-2(f), AC-2(g), AC-2(h), AC-2(i), AC-2(j), AC-2(k), AC-2(l), AC-2(1), AC-2(2), AC-2(3)(a-d), AC-2(4), AC-2(9), AC-2(12)(a), AC-2(12)(b), AC-3

Automatically disable inactive accounts

Disable accounts under each of these conditions:

- Expired: set an expiration date, or use automated disabling, for accounts that should expire on a known date (e.g. contractor/temporary accounts)
- No longer associated with a user: detect and disable orphaned accounts within a defined timeframe
- Policy violation: disable a user's access promptly when they violate your rules of behavior
- Inactive 90 days: configure your IdP to auto-disable after 90 days of inactivity

Covers: AC-2(3)(a-d)

Apply extra controls to privileged accounts

For privileged accounts:

- Set usage conditions for privileged accounts
- Monitor and log privileged account activity
- Disable privileged access when no longer needed
- Apply additional safeguards consistent with your risk policies

Covers: AC-2(7)(a), AC-2(7)(b), AC-2(7)(c), AC-2(7)(d)

Control what data flows in and out

For data moving between your systems and GovOps:

- Define what data types may flow to and from GovOps
- Configure your log shippers and other monitoring systems to use the private key Coralogix issues to you when sending logs and events to GovOps

Covers: AC-4, AC-4(21)

Enforce separation of duties

Define which duties require separation among your personnel, and assign roles accordingly so no one person has all access needed for a critical function alone.

Covers: AC-5(a), AC-5(b)

Apply least privilege

Apply least privilege across your team:

- Limit access to security functions to authorized personnel
- Require non-privileged accounts for non-security, day-to-day work
- Restrict privileged accounts to designated roles
- Retain logs of privileged function use

Covers: AC-6, AC-6(1)(a), AC-6(1)(b), AC-6(2), AC-6(5), AC-6(9)

Configure account logout on your identity provider

Implement and configure account logout settings on your own identity provider for your users. This is separate from and in addition to Coralogix's own account logout on GovOps accounts.

Covers: AC-7(a, b)

Show a system use notification banner

Before your users sign in to GovOps:

- Define and configure a system use notification banner, consistent with federal requirements and your policies
- Keep it on screen until users acknowledge the usage conditions and take explicit action to log in
- Include the required privacy and security notices, and state that the system is subject to monitoring

Covers: AC-8(a), AC-8(b), AC-8(c)

Configure session timeouts

Your GovOps administrators can set two timeouts for your users:

- Activity timeout: logs a user out of a browser window after a set period without interaction. Set it to start within 15 minutes of inactivity
- Force logout: logs a user out after a set period, regardless of activity
- Apply your organization's session timeout policies through your identity provider as well

Covers: AC-2(5), AC-11(a), AC-11(1), AC-12, SC-10

Document any actions allowed without authentication

If any actions in your tenant can be performed without identification or authentication, identify and document the rationale in your security plan. Rare in practice.

Covers: AC-14(a), AC-14(b)

Set rules for remote access

For remote access to GovOps:

- Establish usage rules for remote access
- Authorize remote access before allowing it
- Monitor and control remote access sessions
- Use encryption for the confidentiality of remote sessions on your side
- Route remote access through your own managed network access control points
- Authorize and document the rationale for any privileged commands run over remote access

Covers: AC-17(a), AC-17(b), AC-17(1), AC-17(2), AC-17(3), AC-17(4)(a), AC-17(4)(b)

Set rules for wireless access, if used

If your personnel connect wirelessly, establish usage rules, authorize connections, and require authentication and encryption.

Covers: AC-18(a), AC-18(b), AC-18(1), AC-18(3)

Set rules for mobile devices, if used

If your personnel use mobile devices to access GovOps, set usage rules, authorize devices (e.g. through your MDM solution), and require device encryption.

Covers: AC-19(a), AC-19(b), AC-19(5)

Verify permissions before sharing information

Set up GovOps so your users can confirm a recipient's access matches the information's restrictions before sharing:

- Tag your data: configure your log and event shippers to classify logs and events by "application" and "subsystem"
- Group into scopes: in Coralogix RBAC, group applications and subsystems into scopes, and grant users and groups access only to the scopes their duties require — Coralogix enforces these settings automatically
- Keep a record: maintain a record of which users and groups can access which scopes, and share it with your users so they can make informed sharing decisions

Covers: AC-21(a), AC-21(b)

Control public-facing content, if applicable

If your organization posts information to any publicly accessible part of GovOps:

- Designate who's authorized to post
- Train authorized posters
- Periodically review public content
- Remove any nonpublic information found

Covers: AC-22(a), AC-22(b), AC-22(c), AC-22(d)

Set rules for external systems

For external systems (not owned/controlled by your organization) accessing GovOps:

- Establish terms and conditions for accessing GovOps from external systems
- Establish terms for using external systems to process/store/transmit GovOps-related information
- Verify external systems meet your required security controls before permitting access
- Retain documentation of approved external system connection agreements

Covers: AC-20(a), AC-20(b), AC-20(1)(a), AC-20(1)(b)

Restrict portable storage on external systems

Restrict or prohibit use of your organization's portable storage devices on external systems that connect to GovOps, consistent with your media use policies.

Covers: AC-20(2)

Prevent non-privileged users from executing privileged functions

Ensure your non-privileged personnel cannot execute privileged functions within GovOps, and review logs to detect and respond to any inappropriate or unauthorized attempts to do so.

Covers: AC-6(10)

Periodically review and adjust privileged access

Review the privileges assigned to your personnel at a regular frequency to confirm they're still needed, and reassign or remove any privileges found to be unnecessary or inconsistent with least privilege.

Covers: AC-6(7)(a), AC-6(7)(b)

AT — Awareness and Training

Provide general security awareness training

Train your personnel on:

- Initial & periodic: provide training at onboarding, and refresh it on a recurring schedule
- Event-driven updates: retrain when required by system changes or following an incident
- Insider threat awareness: cover indicators of insider threat
- Social engineering awareness: cover social engineering and social mining tactics

Covers: AT-2(a), AT-2(b), AT-2(c), AT-2(d), AT-2(2), AT-2(3)

Provide role-based training for security-responsible personnel

Train anyone with assigned security responsibilities related to GovOps:

- Initial: before they're granted access or assigned security-related duties
- Event-driven: when required by system changes
- Periodic: on a recurring refresh schedule

Covers: AT-3(a), AT-3(b), AT-3(c)

Document and retain training records

Document training completion for your personnel and retain records for the period your organization requires.

Covers: AT-4(a), AT-4(b)

AU — Audit and Accountability

Define what else needs to be logged

Identify additional logging needs beyond Coralogix's defaults:

- Identify the additional event types your organization needs logged
- Coordinate that logging function across your organization
- Provide a rationale for why each additional event type is needed
- Ensure the components involved actually generate those logs
- Keep this approach consistent across your organization

Covers: AU-2(a), AU-2(b), AU-2(c), AU-2(d), AU-2(e)

Confirm your audit records are complete

Your activity's audit records should capture what happened, when, where, the source, the outcome, and who was involved. This is largely automatic, but worth periodically confirming for your integration.

Covers: AU-3(a), AU-3(b), AU-3(c), AU-3(d), AU-3(e), AU-3(f), AU-3(1)

Manage any audit storage you keep outside GovOps

If you maintain supplemental audit log storage outside the platform, ensure it has sufficient capacity to avoid data loss.

Covers: AU-4

Set up alerts for audit failures

Configure alerts to notify your personnel if audit logging fails, and define what your organization does in response.

Covers: AU-5(a), AU-5(b)

Regularly review your audit logs

Review your tenant's audit logs on a schedule:

- Review and analyze logs for indications of inappropriate activity
- Report findings to the right people
- Adjust the level of review based on risk
- Integrate this into your broader security review process
- Correlate findings across your different audit sources, if you have more than one

Covers: AU-6(a), AU-6(b), AU-6(c), AU-6(1), AU-6(3)

Use audit reduction and reporting tools carefully

If you use tools to analyze or summarize audit data, make sure they don't alter the original records or their time ordering.

Covers: AU-7(a), AU-7(b), AU-7(1)

Confirm audit timestamps meet requirements

Timestamps on your audit records should use UTC/GMT and meet your organization's required precision -- typically automatic, but worth confirming.

Covers: AU-8(a), AU-8(b)

Protect audit data you export or store elsewhere

Protect audit data or tools you export from GovOps:

- Protect it from unauthorized access, modification, or deletion
- Alert your team if that protection is compromised
- Restrict who has privileges to access it

Covers: AU-9(a), AU-9(b), AU-9(4)

Retain audit records per your retention policy

Keep audit records related to your GovOps use for as long as your records retention policy and applicable federal requirements call for.

Covers: AU-11

Ensure custom logging selections generate compliant records

If you've selected additional event types to log or integrated components with GovOps, confirm those generate records that meet the same content standards.

Covers: AU-12(a), AU-12(b), AU-12(c)

CA — Assessment, Authorization, and Monitoring

Assess your own systems periodically

Assess your own systems that connect to GovOps:

- Develop a security assessment plan
- Select an assessor with the required independence
- Conduct the assessment per your plan
- Produce a security assessment report
- Provide the results to the right people in your organization
- You can leverage Coralogix's own FedRAMP assessment results to satisfy inherited-control requirements
- Use specialized assessment techniques as part of your process (e.g. vulnerability scanning, penetration testing, insider threat assessment), announced or unannounced per your risk approach

Covers: CA-2(a), CA-2(b), CA-2(c), CA-2(d), CA-2(e), CA-2(f), CA-2(1), CA-2(3)

Manage interconnections with GovOps

For any formal interconnections between your systems and GovOps:

- Approve and manage the connection
- Document an interconnection security agreement where required
- Review and update the agreement periodically

Covers: CA-3(a), CA-3(b), CA-3(c), CA-9(a), CA-9(b), CA-9(c), CA-9(d)

Maintain a plan of action for your own gaps

Track remediation plans (a POA&M) for any deficiencies found in your own security assessments relevant to your GovOps use, and update it as you close items or find new ones.

Covers: CA-5(a), CA-5(b)

Formally authorize your own systems

Formally authorize your own use of GovOps:

- Have your authorizing official formally authorize your systems
- Reference Coralogix's FedRAMP authorization package as the basis for inherited controls
- Keep that authorization current and re-authorize per your schedule

Covers: CA-6(a), CA-6(b), CA-6(c), CA-6(d), CA-6(e)

Continuously monitor your own controls

Maintain a continuous monitoring program for the controls you implement yourself:

- Define metrics and assessment frequency for your own controls
- Ongoing assessment of your own control effectiveness
- Correlate and analyze findings across your monitoring sources
- Take response actions on what you find
- Report status to the right people in your organization
- Review and update your monitoring strategy periodically

Covers: CA-7(a), CA-7(b), CA-7(c), CA-7(d), CA-7(e), CA-7(f), CA-7(g), CA-7(1), CA-7(4)(a), CA-7(4)(b), CA-7(4)(c)

Conduct your own penetration testing

Periodically test your own systems that connect to GovOps, including independent testing and red-team exercises where consistent with your risk strategy.

Covers: CA-8, CA-8(1), CA-8(2)

CM — Configuration Management

Maintain a baseline configuration for your integration

Maintain a baseline for anything you manage that connects to GovOps (your IdP, API integrations):

- Establish and document a baseline configuration
- Review and update it periodically
- Automate baseline maintenance where possible
- Retain previous versions for rollback

Covers: CM-2(a), CM-2(b), CM-2(2), CM-2(3)

Harden devices used for high-risk travel, if applicable

If personnel travel to high-risk locations, issue devices with approved, hardened configurations, and apply extra safeguards before they reconnect.

Covers: CM-2(7)(a), CM-2(7)(b)

Run a change control process for your integration

For changes to your IdP/API configuration:

- Review proposed changes before implementing them
- Document and approve changes
- Test changes before implementing, ideally in a separate environment
- Retain change records
- Provide oversight (e.g. a change board) for changes affecting your GovOps integration

Covers: CM-3(a), CM-3(b), CM-3(c), CM-3(d), CM-3(e), CM-3(f), CM-3(g), CM-3(2), CM-3(4)

Analyze the security impact of changes before making them

Assess how a proposed change to your integration could affect your security posture, testing in a separate environment first where practical.

Covers: CM-4, CM-4(2)

Restrict who can change your integration configuration

For your IdP/integration configuration:

- Limit who on your team can make changes
- Enforce that restriction through automated access controls where possible
- Limit who has privileges to change production settings
- Periodically review who has change privileges

Covers: CM-5, CM-5(1)(a), CM-5(1)(b), CM-5(5)(a), CM-5(5)(b)

Use secure configuration settings

For your IdP/integration configuration:

- Establish secure configuration settings for the technology you use
- Implement those settings
- Document and approve any necessary deviations
- Monitor for and control unauthorized configuration changes
- Automate configuration management where possible

Covers: CM-6(a), CM-6(b), CM-6(c), CM-6(d), CM-6(1)

Disable unnecessary functions and restrict software

For your IdP/integration configuration:

- Configure components to provide only essential capabilities
- Disable unnecessary ports, protocols, and services
- Periodically review and disable anything no longer needed
- Maintain an allow-list of approved software
- Keep the allow-list current and monitor for compliance

Covers: CM-7(a), CM-7(b), CM-7(1)(a), CM-7(1)(b), CM-7(2), CM-7(5)(a), CM-7(5)(b), CM-7(5)(c)

Maintain an inventory of your integration components

Keep an up-to-date inventory of anything you manage that connects to GovOps (your IdP, API integrations):

- Develop and maintain the inventory
- Review and update it periodically
- Detect and respond to any unauthorized components

Covers: CM-8(a), CM-8(b), CM-8(1), CM-8(3)(a), CM-8(3)(b)

Maintain a configuration management plan

Document how configuration management works for your GovOps-connected components -- roles, responsibilities, what counts as a configuration item, and how the plan itself is protected from unauthorized changes.

Covers: CM-9(a), CM-9(b), CM-9(c), CM-9(d), CM-9(e)

Control what software your users can install

For devices your users use to access GovOps:

- Set policy on what software users may install
- Enforce that policy
- Periodically check compliance

Covers: CM-11(a), CM-11(b), CM-11(c)

Track where your sensitive information lives

For your GovOps tenant:

- Identify and document what types of information you process
- Document where that information flows within your environment and GovOps
- Document any restrictions on how it flows
- Keep this current, using automated tools where possible

Covers: CM-12(a), CM-12(b), CM-12(c), CM-12(1)

Respect software licensing and copyright

For software connected to your GovOps integration:

- Use it in accordance with license agreements and copyright law
- Track license quantities where applicable
- Control and document any use of peer-to-peer file-sharing technology

Covers: CM-10(a), CM-10(b), CM-10(c)

CP — Contingency Planning

Maintain a contingency plan

Document a contingency plan covering your dependency on GovOps:

- Develop it and get it approved by the right people in your organization
- Coordinate it with your other plans (business continuity, disaster recovery, incident response)
- Define roles and responsibilities for contingency operations
- Address how you'll maintain essential functions during a disruption, and fully restore afterward
- Define how quickly you need to resume essential functions
- Identify the critical assets that support those essential functions
- Protect the plan from unauthorized disclosure, and share it with key personnel

Covers: CP-2(a), CP-2(b), CP-2(c), CP-2(d), CP-2(e), CP-2(f), CP-2(g), CP-2(h), CP-2(1), CP-2(3), CP-2(8)

Train personnel on contingency procedures

Train anyone with a contingency role, within a defined time of them taking on that role and again whenever your procedures change.

Covers: CP-3(a), CP-3(b)

Test your contingency plan regularly

Test your contingency plan on a schedule:

- Run the test
- Review the results
- Initiate corrective actions for anything that failed
- Coordinate testing with your other related plans

Covers: CP-4(a), CP-4(b), CP-4(c), CP-4(1)

Secure and test any alternate sites or backups you maintain

If your organization maintains its own alternate storage, alternate processing, or backups related to your GovOps use:

- Alternate storage site: establish it, separate it from your primary site to avoid shared risks, and address any accessibility concerns
- Alternate processing site: establish it with agreements for availability, resources consistent with your recovery time objective, and separation from your primary site
- Backups: back up user data, system data, and documentation; protect their confidentiality, integrity, and availability (including cryptographically); and test them periodically for reliability

Covers: CP-6(a), CP-6(b), CP-6(1), CP-6(3), CP-7(a), CP-7(b), CP-7(c), CP-7(1), CP-7(2), CP-7(3), CP-9(a), CP-9(b), CP-9(c), CP-9(d), CP-9(1), CP-9(8)

Maintain alternate connectivity

Establish backup telecommunications service so you can keep reaching GovOps if your primary connectivity fails:

- Arrange agreements that include priority-of-service provisions
- Request the priority service
- Ensure the backup service has adequate protection and doesn't share a single point of failure with your primary connection

Covers: CP-8, CP-8(1)(a), CP-8(1)(b), CP-8(2)

Maintain your own recovery capability

Maintain your own ability to recover and restore your systems to a known, secure state after a disruption affecting your GovOps use, consistent with your contingency plan. If your integration involves transaction-based processing, implement mechanisms to recover and roll back incomplete or failed transactions.

Covers: CP-10, CP-10(2)

IA — Identification and Authentication ▼

Configure your identity provider correctly

Set up a SAML 2.0 identity provider, and configure your GovOps account to trust it to make identification and authentication decisions:

- Uniquely identify and authenticate each of your users
- Identify and authenticate non-organizational users (e.g. contractors, partners, or users from other agencies) who access your tenant

Covers: IA-2, IA-8

Enforce MFA for every account

Require multi-factor authentication for your accounts:

- Require MFA for privileged accounts over the network
- Require MFA for non-privileged accounts over the network
- Require individual authentication before granting access to any shared/group credential
- Make sure at least one authentication factor comes from a device separate from the one being used to sign in
- Use replay-resistant authentication methods for privileged network access

Covers: IA-2(1), IA-2(2), IA-2(5), IA-2(6)(a), IA-2(6)(b), IA-2(8)

Support PIV/CAC federation, if required

If your organization requires it, configure your IdP to (setup guide: coralogix.com/docs/sso-with-saml):

- Accept and electronically verify PIV/CAC smart cards, including HSPD-12 requirements and PIV credentials issued by other agencies
- Define the CA server that supports your HSPD-12 implementation
- Accept only FICAM-approved third-party credentials, using only FICAM-approved components to accept them
- Conform to FICAM-issued profiles

Covers: IA-2(12), IA-8(1), IA-8(2)(a, b), IA-8(4)

Uniquely identify connecting devices, if applicable

If your device management policies require it, uniquely identify devices before they connect to GovOps.

Covers: IA-3

Manage user identifiers

Manage identifiers in your IdP:

- Get authorization before assigning a new identifier
- Select a unique identifier for each user
- Prevent reuse of an identifier for a defined period
- Disable an identifier after a defined period of inactivity
- Uniquely identify each individual as an employee, contractor, or other category

Covers: IA-4(a), IA-4(b), IA-4(c), IA-4(d), IA-4(4)

Administer your own authentication requirements

Administer authentication for your users:

- Verify each user's identity before creating their account
- Set initial credentials and ensure they meet strength requirements
- Set password complexity and character-change requirements
- Handle lost, compromised, or damaged authenticators; set password lifetime limits and prevent reuse; allow temporary passwords with forced change
- Protect authenticator content from unauthorized disclosure or modification

Covers: IA-5(a), IA-5(b), IA-5(c), IA-5(d), IA-5(f), IA-5(1)(a), IA-5(1)(b, d), IA-5(1)(e), IA-5(1)(f), IA-5(1)(g, h)

Validate PKI certificates, if used

If using PKI-based authentication, make sure your IdP accepts and electronically verifies it:

- Validate certificates by building and verifying a certification path to a trusted anchor, including checking revocation status
- Enforce authorized access to the corresponding private keys
- Map each authenticated identity to the right individual or group account
- Keep a local cache of revocation data so validation still works if the network is unavailable

Covers: IA-5(2)(a), IA-5(2)(b)

Protect credentials

Use approved tools (e.g. password managers) so authenticators aren't stored or transmitted in cleartext, and never embed static credentials in scripts or applications.

Covers: IA-5(6), IA-5(7)

Obscure authentication feedback and use compliant cryptography

Ensure your IdP doesn't display authentication details that could be exploited, and that authentication uses FIPS-validated cryptographic modules.

Covers: IA-6, IA-7

Require re-authentication under defined conditions

Configure your IdP to require users to re-authenticate after inactivity or privilege escalation.

Covers: IA-11

Verify your users' identities before granting access

Verify each user's identity before granting access:

- Identity-proof users
- Resolve their claimed identity to a specific, unique individual
- Validate the identity evidence they provide
- Proof at Identity Assurance Level 2 or higher
- Validate/verify identity evidence through defined methods
- Have a process for supervisor or representative involvement when direct physical presence isn't feasible

Covers: IA-12(a), IA-12(b), IA-12(c), IA-12(2), IA-12(3), IA-12(5)

IR — Incident Response

Train personnel on incident response

Train anyone with an incident response role, particularly on how to report incidents involving GovOps, and retrain when your procedures change.

Covers: IR-2(a), IR-2(b)

Test your incident response capability

Test your incident response procedures on a schedule, incorporating lessons learned, and coordinate that testing with your other related plans.

Covers: IR-3, IR-3(2)

Maintain an incident handling capability

Maintain your own incident handling capability:

- Cover preparation, detection, analysis, containment, eradication, and recovery
- Coordinate it with your contingency planning
- Incorporate lessons learned from past incidents
- Ensure it's effective and applied consistently
- Use automated tools to support incident handling where possible

Covers: IR-4(a), IR-4(b), IR-4(c), IR-4(d), IR-4(1)

Track and document incidents

Keep records of any incidents affecting your GovOps tenant.

Covers: IR-5

Report suspected incidents to Coralogix immediately

Report incidents involving GovOps:

- Email the Coralogix Security Operations Team at security@coralogix.com as soon as an incident is suspected
- Your organization is the final approval authority for system use -- if your agency learns of an incident Coralogix hasn't yet reported, you must notify Coralogix, US-CERT, and FedRAMP stakeholders yourself
- Make sure your agency-specific incident response plan requirements are met
- For Agency Authorizations, confirm Coralogix obtained a US-CERT tracking number

Covers: IR-6(a), IR-6(b), IR-6(1), IR-6(3)

Provide an incident support resource for your personnel

Give your personnel a place to get advice on handling and reporting GovOps-related incidents, using automated support tools where possible.

Covers: IR-7, IR-7(1)

Maintain a written incident response plan

Maintain a written incident response plan:

- Develop it
- Distribute it to key personnel
- Review and get it approved
- Communicate changes when it's updated
- Protect it from unauthorized disclosure

Covers: IR-8(a), IR-8(b), IR-8(c), IR-8(d), IR-8(e)

Have an information-spill response procedure

Maintain an information-spill response procedure for anything involving your GovOps tenant:

- Assign responsibility for responding to spills
- Identify what information was involved
- Alert the right personnel
- Isolate and eradicate the spilled data
- Handle the spilled information per applicable policies, and implement measures to prevent recurrence
- Train personnel on spill response, and define post-spill operating procedures
- Limit exposure to personnel who don't need access to the spilled information

Covers: IR-9(a), IR-9(b), IR-9(c), IR-9(d), IR-9(e), IR-9(f), IR-9(g), IR-9(2), IR-9(3), IR-9(4)

PL — Planning

Maintain your own system security plan

Maintain a system security plan for your own systems:

- Explicitly define your authorization boundary
- Describe the operational context your system runs in
- Provide a security categorization and the rationale behind it
- Describe the controls in place or planned -- including which are inherited from GovOps
- Keep it aligned with your enterprise architecture

Covers: PL-2(a), PL-2(b), PL-2(c), PL-2(d), PL-2(e)

Establish and enforce rules of behavior

Establish rules of behavior for your users:

- Establish the rules, including explicit restrictions on social media use, posting to external sites, and sharing CUI/PII
- Restrict personal device use where applicable
- Get signed acknowledgment from users before authorizing access
- Review and update the rules periodically, and re-acknowledge when they change

Covers: PL-4(a), PL-4(b), PL-4(c), PL-4(d), PL-4(1)(a), PL-4(1)(b), PL-4(1)(c)

Maintain your own security architecture documentation

Document your own security architecture:

- Describe how it meets your security and privacy requirements
- Describe how it integrates with your enterprise architecture
- Describe any risk management decisions behind it

Covers: PL-8(a), PL-8(b), PL-8(c)

Tell Coralogix which webhook destinations you've approved

If you send GovOps alerts to your own systems through webhooks, give Coralogix the list of approved network targets, and let us know when it changes. FedRAMP requires every external network connection to be documented, so Coralogix adds these targets to the GovOps security architecture.

Covers: PL-8(a)

Document how your control baseline is satisfied

Select an appropriate control baseline for your own systems, commensurate with their security categorization, and document how controls inherited from GovOps satisfy that baseline.

Covers: PL-11, PL-10

PS — Personnel Security

Assign risk designations to positions

For any position requiring GovOps access:

- Assign a risk designation to the position
- Establish screening criteria appropriate to that risk level
- Review and update designations periodically

Covers: PS-2(a), PS-2(b), PS-2(c)

Screen personnel before granting access

Before granting GovOps access:

- Screen the individual
- Rescreen per your defined conditions and frequency
- Verify security clearances, if applicable
- Ensure signed nondisclosure agreements are in place, if applicable

Covers: PS-3(a), PS-3(b), PS-3(3)(a), PS-3(3)(b)

Offboard departing personnel promptly

When someone leaves or their access should end:

This typically follows a 4-hour disable window (1 hour for privileged access) from notification, per your defined procedure.

- Disable their access
- Terminate or revoke their credentials and authenticators
- Conduct an exit interview covering security obligations
- Retrieve any security-related organizational property
- Retain appropriate access to information/systems formerly under their control

Covers: PS-4(a), PS-4(b), PS-4(c), PS-4(d), PS-4(e)

Update access when personnel change roles

When someone changes roles:

- Review whether their access is still needed
- Initiate access changes within your defined timeframe
- Modify access as needed
- Notify the right people of the change

Covers: PS-5(a), PS-5(b), PS-5(c), PS-5(d)

Use signed access agreements

For access agreements:

- Have personnel sign one before authorizing access
- Review and update the agreement periodically
- Retain signed copies

Covers: PS-6(a), PS-6(b), PS-6(c)

Hold third parties to your security requirements

If contractors or third-party providers access your tenant:

- Establish personnel security requirements for them
- Document those requirements in contracts
- Require their compliance
- Monitor their ongoing compliance
- Require notification when their personnel transfer or terminate

Covers: PS-7(a), PS-7(b), PS-7(c), PS-7(d), PS-7(e)

Have a sanctions process for policy violations

Apply consequences for personnel who violate your security policies, and notify the right managers when that happens.

Covers: PS-8(a), PS-8(b)

Include security responsibilities in job descriptions

Reflect security and privacy responsibilities in the position descriptions of anyone who accesses or administers GovOps.

Covers: PS-9

RA — Risk Assessment ▼

Categorize your systems and data

Categorize your systems and the information you process through GovOps:

- Categorize per FIPS 199
- Document the results in your security plan
- Get the categorization decision reviewed and approved by your authorizing official

Covers: RA-2(a), RA-2(b), RA-2(c)

Conduct and maintain risk assessments

Assess risk related to your GovOps dependency:

- Conduct the assessment, identifying threats and vulnerabilities
- Integrate current threat intelligence
- Document the results
- Review the results periodically
- Share results with the right people in your organization
- Update the assessment periodically or when significant changes occur

Covers: RA-3(a), RA-3(b), RA-3(c), RA-3(d), RA-3(e), RA-3(f)

Assess supply chain risk

Assess supply chain risks associated with your use of GovOps as part of your own risk management process, including risk from the cloud service supply chain, and document and incorporate the results into your risk decisions.

Covers: RA-3(1)(a), RA-3(1)(b)

Scan your own components for vulnerabilities

Scan whatever you manage that connects to GovOps (your IdP, integrations):

- Scan periodically and whenever new vulnerabilities are identified
- Use scanning tools that check for known flaws, misconfigurations, and missing patches
- Analyze scan reports
- Remediate confirmed vulnerabilities within your response-time requirements
- Share findings that could help eliminate similar vulnerabilities elsewhere
- Keep your scanning tools updated, sized to adequate coverage, and use privileged access where needed for accurate results

Covers: RA-5(a), RA-5(b), RA-5(c), RA-5(d), RA-5(e), RA-5(f), RA-5(2), RA-5(3), RA-5(5), RA-5(11)

Act on assessment and monitoring findings

Respond to findings from your security assessments and risk monitoring consistent with your risk management process.

Covers: RA-7

Identify critical components for resilience planning

Identify which of your own components are critical to your GovOps use and factor that into your resilience and supply chain planning.

Covers: RA-9

SA — System and Services Acquisition ▼

Budget and plan for security

Include security requirements in your mission planning and budgeting for any systems that use GovOps.

Covers: SA-2(a), SA-2(b), SA-2(c)

Follow a secure development lifecycle, if you build integrations

If your organization develops custom systems that connect to GovOps, incorporate security throughout the development lifecycle with clearly assigned roles.

Covers: SA-3(a), SA-3(b), SA-3(c), SA-3(d)

Include security requirements in procurement contracts

When acquiring systems or services that will connect to GovOps, include in the contract:

- Security and privacy functional requirements
- Documentation requirements
- Development process, standards, and tools to be used
- Acceptance criteria
- Requirements for identifying functions/ports/protocols/services used

Covers: SA-4(a), SA-4(b), SA-4(c), SA-4(d), SA-4(e), SA-4(f), SA-4(g), SA-4(h), SA-4(i), SA-4(1), SA-4(2), SA-4(9)

Maintain documentation for your integration components

Maintain documentation for anything you manage that connects to GovOps:

If documentation is unavailable or nonexistent, document that fact and your response.

- Obtain or develop administrator documentation
- Obtain or develop user documentation
- Protect documentation per your classification policy

Covers: SA-5(a), SA-5(b), SA-5(c), SA-5(d)

Apply security engineering principles

Apply sound security and privacy engineering practices when specifying, building, or modifying anything that connects to GovOps.

Covers: SA-8

Oversee external service providers

For any external services connected to your GovOps tenant:

- Require them to meet your security requirements
- Monitor their ongoing compliance
- Establish and maintain trust relationships with them based on your own defined criteria

Covers: SA-9(a), SA-9(b), SA-9(c), SA-9(1)(a), SA-9(1)(b), SA-9(2)

Restrict where your information is processed

If applicable, restrict the locations where information related to your GovOps use is processed and stored.

Covers: SA-9(5)

Test custom integrations for security flaws, if you build them

If you develop custom systems that connect to GovOps:

- Require testing, threat modeling, and flaw remediation before deployment
- Use static code analysis tools to identify common flaws, and document the results

Covers: SA-11(a), SA-11(b), SA-11(c), SA-11(d), SA-11(e), SA-11(1), SA-11(2)(a), SA-11(2)(b), SA-11(2)(c), SA-11(2)(d)

Follow a documented development process, if applicable

Require your developers to follow a documented process addressing security requirements, and periodically review that process.

Covers: SA-15(a), SA-15(b), SA-15(3)(a), SA-15(3)(b)

Replace or justify unsupported components

Replace components that connect to GovOps once they're no longer supported, or document approved compensating controls if you continue using them.

Covers: SA-22(a), SA-22(b)

Use approved PIV products and set up federation, if applicable

If your organization uses PIV-based authentication for GovOps:

- Use only PIV card products on the FIPS 201-approved products list that can integrate with GovOps SSO through SAML or another trusted identity provider
- Set up identity federation so your organization can use PIV/CAC cards to access GovOps (setup guide: coralogix.com/docs/ssso-with-saml)

Covers: SA-4(10)

SC — System and Communications Protection

Separate admin functions from general user access

On anything you manage that connects to GovOps, keep administrative interfaces separate from general user functionality.

Covers: SC-2

Prevent data leakage between sessions

Prevent unintended information transfer between sessions or users:

- Configure Coralogix RBAC according to least privilege, so each user can only reach the data their role requires
- Ensure shared resources on your side don't allow unintended information transfer

Covers: SC-4

Protect against denial-of-service attacks

Implement DoS protections -- rate limiting, traffic filtering -- on the infrastructure you manage that connects to GovOps.

Covers: SC-5(a), SC-5(b)

Protect your network boundary

For your own network boundary:

- Monitor and control communications at your network boundary and key internal boundaries
- Route through managed interfaces only, with documented traffic-flow policies -- justify and periodically review any exceptions
- Apply deny-by-default, allow-by-exception traffic rules
- Don't allow split tunneling for remote devices; route internal traffic through an authenticated proxy where required
- Isolate your own security tools and support components from other internal components
- Limit external network connections, and use host-based boundary protection where appropriate
- Ensure your boundary protection devices fail secure, not open

Covers: SC-7(a), SC-7(b), SC-7(c), SC-7(3), SC-7(4)(a), SC-7(4)(b), SC-7(4)(c), SC-7(4)(d), SC-7(4)(e), SC-7(4)(f), SC-7(4)(g), SC-7(4)(h), SC-7(5), SC-7(7), SC-7(8), SC-7(12), SC-7(18)

Encrypt data in transit and validate GovOps certificates

Protect data moving between your systems and GovOps:

- Use FIPS-validated cryptography
- Configure your systems to validate the Coralogix US GovOps public certificates, so data is never sent to an attacker impersonating GovOps (a man-in-the-middle attack)

Covers: SC-8, SC-8(1), SC-23

Manage cryptographic keys and use approved cryptography

For cryptographic keys you manage:

- Establish and manage keys per federal requirements
- Use FIPS-compliant key management for symmetric keys
- Use FIPS-compliant key management for asymmetric keys
- Use only FIPS-validated or NSA-approved cryptography, documented

Covers: SC-12, SC-13(a), SC-13(b)

Control collaborative computing devices

Prohibit remote activation of cameras/microphones except where explicitly authorized, with a clear in-use indicator.

Covers: SC-15(a), SC-15(b)

Manage certificates and trust stores

Issue or obtain approved public key certificates, and include only approved trust anchors in your trust stores.

Covers: SC-17(a), SC-17(b)

Control mobile code

Define what mobile code is acceptable, and authorize and monitor its use.

Covers: SC-18(a), SC-18(b)

Verify DNS integrity

Verify data origin and integrity of name-resolution responses, and ensure your name resolution service is fault-tolerant.

Covers: SC-21, SC-22

Encrypt data at rest

Protect the confidentiality and integrity of information at rest in anything you manage that supports your GovOps tenant — including any AWS S3 buckets in your own AWS account that store your GovOps logs. Coralogix protects data at rest in its own AWS account.

Covers: SC-28, SC-28(1)

Secure the S3 buckets that store your logs

For the AWS S3 buckets in your own AWS account where GovOps stores your logs:

- Create the buckets GovOps will write your logs to
- Set the bucket policy and IAM permissions so only Coralogix US GovOps and your authorized users and use cases can access them
- Protect the data at rest in those buckets, e.g. with encryption

Covers: SC-4, SC-28, SC-28(1)

Maintain process isolation

Keep separate execution domains for processes on systems that connect to GovOps.

Covers: SC-39

Synchronize system clocks

Keep your system clocks synchronized to an authoritative time source, checking regularly for drift.

Covers: SC-45, SC-45(1)(a), SC-45(1)(b)

SI — System and Information Integrity ▼

Patch your own systems promptly

For anything you manage that connects to GovOps:

- Identify applicable security updates
- Test updates before installing
- Install updates within your defined timeframe
- Track how long remediation takes

Covers: SI-2(a), SI-2(b), SI-2(c), SI-2(d), SI-2(2), SI-2(3)(a), SI-2(3)(b)

Run malware protection

Detect and block malicious code at entry/exit points of your systems, keeping protection mechanisms updated.

Covers: SI-3(a), SI-3(b), SI-3(c), SI-3(d)

Monitor your systems for attacks

Monitor whatever you manage that connects to GovOps:

- Monitor for attacks and unauthorized connections, using strategically deployed tools
- Protect monitoring information from unauthorized access, and adjust monitoring intensity based on risk (get legal review of your monitoring activities where required)
- Use automated, real-time analysis tools, including intrusion detection/prevention integrated into your broader monitoring
- Monitor inbound/outbound traffic for unusual or unauthorized activity, including signs of data exfiltration
- Alert on indicators of compromise
- Correlate monitoring information across your different sources, and use host-based monitoring where relevant

Covers: SI-4(a), SI-4(b), SI-4(c), SI-4(d), SI-4(e), SI-4(f), SI-4(g), SI-4(1), SI-4(2), SI-4(4)(a), SI-4(4)(b), SI-4(5), SI-4(16), SI-4(18), SI-4(23)

Act on security alerts and advisories

Receive alerts from sources like US-CERT, distribute them internally, and implement required directives on schedule.

Covers: SI-5(a), SI-5(b), SI-5(c), SI-5(d)

Verify security functions work correctly

Periodically confirm your security controls are operating as expected, and alert and respond when anomalies show up.

Covers: SI-6(a), SI-6(b), SI-6(c), SI-6(d)

Detect unauthorized changes

Use integrity verification tools to catch unauthorized changes to your software or data, and feed detections into your incident response process.

Covers: SI-7(a), SI-7(b), SI-7(1), SI-7(7)

Run spam protection

Protect email systems used by personnel who access GovOps, kept up to date and centrally managed.

Covers: SI-8(a), SI-8(b), SI-8(2)

Manage information retention

Retain information within your tenant per your records management policy and applicable federal requirements.

Covers: SI-12

Protect system memory

Enable available protections against unauthorized code execution on systems that connect to GovOps.

Covers: SI-16

Validate data before submission

If your organization submits data to GovOps through custom scripts, integrations, or automated pipelines, validate that the data conforms to expected formats before submission to reduce the risk of malformed or malicious input.

Covers: SI-10

Handle error messages safely

In systems you manage that connect to GovOps, make sure error messages give users what they need to fix a problem without revealing information an attacker could exploit, and show detailed errors only to designated personnel.

Covers: SI-11(a), SI-11(b)

SR — Supply Chain Risk Management



Maintain a supply chain risk management plan

Document how you manage supply chain risk for systems connected to GovOps:

- Develop the plan
- Review and update it periodically
- Protect it from unauthorized disclosure
- Coordinate it with your other security and risk management processes

Covers: SR-2(a), SR-2(b), SR-2(c), SR-2(1)

Address supply chain weaknesses

Identify and address weaknesses in your supply chain, document the controls you use, and reflect them in your security plan.

Covers: SR-3(a), SR-3(b), SR-3(c)

Use secure acquisition practices

Apply acquisition strategies and procurement methods that protect against supply chain risk.

Covers: SR-5

Assess your suppliers

Evaluate third-party providers connected to your GovOps tenant to identify supply chain risk.

Covers: SR-6

Require compromise notification from suppliers

Establish agreements requiring your suppliers to notify you of supply chain compromises and assessment results.

Covers: SR-8

Guard against counterfeit components

For components you use:

- Detect and report suspected counterfeit components
- Train personnel to recognize them
- Maintain configuration control over components awaiting service, repair, or return to service

Covers: SR-11(a), SR-11(b), SR-11(1)

Securely dispose of retired components

Sanitize information before disposing of components that were used in connection with GovOps.

Covers: SR-12, SR-11(2)

Inspect systems and components for tampering

Physically and technically inspect systems and components you acquire for use in connection with GovOps at appropriate points in their lifecycle, to detect tampering.

Covers: SR-10
