COMPETITIVE ANALYSIS

Analog Informatics vs. FedRAMP Cloud Services - Competitive Analysis

Compare customer-operated AIC software with FedRAMP cloud services: service boundaries, privileged controls, secret custody and disconnected mission needs.

Revised: November 20, 2026

Analog Informatics Corporation

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Revised November 20, 2026

Strengths and customer fit

Where AIC fits

AIC gives your team direct control of managed secrets, approved administration and operating evidence on the systems it manages. The software can run on your premises, in your cloud account, across a hybrid design or inside a disconnected mission boundary.

Suitable customers: Teams that need to control privileged accounts and corrective work on customer systems, especially when local operators, hybrid infrastructure or air-gapped execution are required.

Where the alternative fits

An appropriate cloud service can provide infrastructure or application operations, a defined authorization boundary and evidence for the provider’s controls. Those services can reduce work the customer would otherwise perform for its own hosting environment.

Suitable customers: Organizations that need the specific infrastructure or application service and authorization boundary. They may host AIC there when the workload and contractual requirements fit.

Who controls deployment and secrets?

Would you delegate control of your most sensitive systems and secrets without knowing who can administer them, where those people are located, and who is accountable for their actions?

AIC is installed where you choose and managed by you. Your organization controls who may use, retrieve or change its managed secrets. Choosing cloud or hybrid infrastructure does not require you to give an outside SaaS operator control of those decisions.

Run AIC on premises, in a cloud account you control, in a hybrid environment, or on air-gapped systems for sensitive missions. You choose where the software runs, who administers it and who may use, retrieve or change the secrets it manages. AIC has no standing access to your installation. Air-gapped deployments can be installed, licensed and updated without a network connection to AIC.

For sensitive work, the server's location is only part of the decision. Your organization chooses the people and approved providers that administer AIC, where they work and which secrets they may access. You control any support access you grant. Cloud infrastructure permissions, local identity services, audit storage, backups and recovery copies remain part of the deployment you choose.

A German operation can install and manage AIC in Germany, while a French operation does the same in France. Each country team can retain control of its secrets and decide which records it shares with the wider organization. This supports country-specific contracts and operating requirements. If a contract or policy requires particular records to stay in the country, include any logs, backups and recovery copies that contain those records.

Related AIC guidance: Air-gapped operation · Security and customer control · Hosting and operating responsibilities

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Deployment comparison

Management service

Analog Informatics: Customer-operated installable software; on-premises, customer-cloud or hybrid.

FedRAMP cloud services: It can be infrastructure, a platform, an application or another provider-operated service. FedRAMP status does not make all services the same delivery model or define customer software operations.

Customer hardware or cloud account

Analog Informatics: The customer chooses supported hardware or cloud systems and its approved administrators.

FedRAMP cloud services: Customers normally consume the provider's defined service. Some products have local variants, but a local installation is not automatically the same authorized service or boundary; establish the exact offering.

Disconnected mission

Analog Informatics: Air-gapped installation, licensing and updates without a network connection to AIC; local dependencies and transfer procedures remain part of the design.

FedRAMP cloud services: A provider-connected service cannot be assumed to run as a standalone disconnected installation. For an isolated mission, identify a documented local product and test its operation without external service access.

Secret and evidence custody

Analog Informatics: Customer-controlled installation and selected storage, including logs, recordings, exports and backups.

FedRAMP cloud services: The actual service, region, logging configuration, exports and backups determine record locations. Include provider control-plane data and support access rather than examining customer storage alone.

Support and operator access

Analog Informatics: The customer decides which administrators or approved providers get access and controls any support access it grants.

FedRAMP cloud services: The named service's access controls, support process, contracts and personnel arrangements determine provider access. Identify which entities and operators can obtain access and from which locations.

Country-local operation

Analog Informatics: The customer can install and manage software in its selected country and include backups, support and recovery in the data map.

FedRAMP cloud services: Evaluate the exact service, operators, locations, record copies and support arrangement; do not infer access control from a provider address or cloud region alone.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Provider independence

Analog Informatics: Retain usable exports, independent emergency access and tested backups; licensed operation still depends on an active license.

FedRAMP cloud services: Provider acquisition or contract changes can affect service continuity and access. Preserve usable exports, customer-owned records and a tested transition plan; negotiate any continuity rights the mission requires.

CQ01 · Alternatives and switching

What are the best alternatives to FedRAMP cloud services?

Analog Informatics: AIC is a strong shortlist choice when you need customer-deployed privileged security and continuous compliance across on-premises and cloud assets. Select alternatives by the job: operating controls, managed services, content collaboration or enterprise governance. A single universal winner would hide those differences.

FedRAMP cloud services: Alternatives include another service with the required boundary, customer-operated infrastructure or a different control platform. AIC can manage customer workloads without replacing the infrastructure service itself.

AIC references: supported platforms · requirements mapping

CQ02 · Alternatives and switching

Which companies compete with FedRAMP cloud services?

Analog Informatics: AIC competes with privileged-access platforms and overlapping security/GRC software, and with the software portion of CMMC enclave offerings. Infrastructure providers and independent assessors can also be partners in an AIC deployment; they are not interchangeable replacements.

FedRAMP cloud services: This category includes many infrastructure and application suppliers. Compare named services and their exact authorization boundaries; a company’s broader portfolio is not one interchangeable FedRAMP offering.

AIC references: supported platforms · requirements mapping

CQ03 · Alternatives and switching

How does AIC compare with FedRAMP cloud services?

Analog Informatics: Treat the cloud service and AIC as separate layers; replacing a provider’s infrastructure is different from replacing a privileged-control tool. AIC combines discovery and management of human and non-human identities with controlled access, automated collection, remediation and reporting. Passwords, SSH keys, certificates and API keys are in scope. Customers retain control of the deployed environment, credentials and evidence.

FedRAMP cloud services: A FedRAMP cloud service supplies its defined service and provider controls. AIC supplies customer-operated security functions for the managed workload; its software role does not duplicate the cloud authorization.

AIC references: supported platforms · requirements mapping

CQ04 · Alternatives and switching

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Can AIC replace FedRAMP cloud services, or do I need both?

Analog Informatics: Replace overlapping functions after proving the required workload and preserving records. Retain a useful external GRC program, content service, cloud platform or MSP where it still does work you need. AIC can supply operational evidence to a wider program through supported interfaces and agreed mappings.

FedRAMP cloud services: Often both are appropriate. Retain the cloud infrastructure or application service you need, and use AIC for customer responsibilities such as privileged accounts, approved sessions and operating evidence.

AIC references: supported platforms · requirements mapping

CQ05 · Alternatives and switching

Why would I switch from FedRAMP cloud services?

Analog Informatics: Switch when customer control, automated corrective action, privileged access or consolidation solves a demonstrated operating problem. A new logo alone is not a reason. Show the improvement on one real workflow before changing production access.

FedRAMP cloud services: Change a cloud service when its workload, contract, access model or boundary no longer fits. Add or change AIC for the customer's operating controls; these are separate purchasing decisions.

AIC references: supported platforms · requirements mapping

CQ06 · Alternatives and switching

Is there a self-hosted alternative to FedRAMP cloud services?

Analog Informatics: Yes. AIC is commercial software deployed in your environment, on-premises or in your own cloud account. Its documented hosting options include disconnected deployments. Other vendors may also offer self-hosting; compare the actual edition.

FedRAMP cloud services: AIC can run on customer hardware or supported customer-cloud systems. Replacing an authorized cloud service with local infrastructure also transfers hosting responsibilities and requires its own suitable design.

AIC references: supported platforms · requirements mapping

CQ07 · Alternatives and switching

Can I replace several security tools with one platform?

Analog Informatics: AIC can consolidate privileged credentials, access, configuration remediation and security-compliance evidence with built-in GRC. Package entitlements matter. Broader corporate governance, specialist collaboration and staffed services may remain separate purchases.

FedRAMP cloud services: Cloud services may bundle infrastructure functions, and AIC may consolidate customer security functions. Retire a specific tool only after locating its replacement in the provider/customer responsibility map.

AIC references: supported platforms · requirements mapping

CQ08 · Alternatives and switching

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

What will I lose-and gain-by switching?

Analog Informatics: You gain a customer-operated path from identity discovery through security action to evidence. You may give up vendor-specific connectors, hosted operations or governance features if you retire them. Inventory those dependencies and retain useful functions until the replacement is proven.

FedRAMP cloud services: Leaving a provider may transfer infrastructure operation and evidence duties to your team. Adding AIC can improve control of managed secrets and actions; it does not recreate the provider's entire service.

AIC references: supported platforms · requirements mapping

CQ09 · Capabilities and coverage

Does this solution solve my whole problem, or only part of it?

Analog Informatics: AIC supplies an integrated security platform and CMMC kits. People still own risk decisions, policies, physical practices and customer-specific operation. Choose the product and scope that cover your technical work; do not equate a software package with every organizational duty.

FedRAMP cloud services: The service covers only its defined boundary and customer configuration. Customer workloads, identities, applications and organizational practices still need assigned controls and evidence.

AIC references: supported platforms · requirements mapping

CQ10 · Capabilities and coverage

Which features are included, and which require another product?

Analog Informatics: Enterprise packages and CMMC levels have different inclusions. The CMMC Level 2 list includes PIM, PAM, PUM, IGA, audit, secure sharing, training/attestation and application launch; Level 1 has a narrower scope. Enterprise audit/training entitlements vary by edition. Use the current product price list for the exact order.

FedRAMP cloud services: Included functions are service-specific. An infrastructure service, collaboration application and managed desktop offering have different boundaries, options and customer duties; use the named service description and order.

AIC references: supported platforms · requirements mapping

CQ11 · Capabilities and coverage

Does it manage both on-premises and cloud systems?

Analog Informatics: Yes. AIC discovers and manages credentials on connected devices, applications, systems, websites and web services across on-premises and cloud environments. Integration kits support management of most on-premises and cloud systems and infrastructure. Customers retain control of the deployed platform, credentials and evidence.

FedRAMP cloud services: Some services manage on-premises resources through supported connections; others only supply cloud functions. Identify where the management service runs and which customer targets it can actually control.

AIC references: supported platforms · requirements mapping

CQ12 · Capabilities and coverage

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Does it support Windows, Linux, network devices, and legacy systems?

Analog Informatics: AIC provides integration kits to manage most on-premises and cloud systems and infrastructure. Documented targets include Windows, Linux/Unix/macOS, AD/LDAP, databases, cloud identities, Cisco, ESXi and management controllers, with browser automation and scripts extending integration to websites, web services and other systems. Match the integration kit and supported operations to the specific device, application, version and protocol.

FedRAMP cloud services: An infrastructure service may host multiple operating systems without managing every guest account or device. Application and management services have their own supported versions, protocols and responsibilities.

AIC references: supported platforms · requirements mapping

CQ13 · Capabilities and coverage

Does it discover accounts and credentials I don’t know about?

Analog Informatics: Yes. AIC discovers human and non-human accounts and credentials across connected devices, applications, systems, websites and web services, on-premises and in cloud environments. Integration kits connect discovery and credential management to the target systems. Review discovered ownership and dependencies before applying changes.

FedRAMP cloud services: Cloud resource inventory does not necessarily discover privileged credentials inside each workload. Compare the actual identity sources, permissions and discovery results before assigning that function to the provider.

AIC references: supported platforms · requirements mapping

CQ14 · Capabilities and coverage

Does it manage non-human identities, service accounts, and AI-agent credentials?

Analog Informatics: Yes. AIC manages non-human identities and their credentials alongside human identities. For an AI agent, identify its actual account, API key or certificate and its target service. Managing that identity is distinct from claiming a native connector to every AI runtime.

FedRAMP cloud services: The provider may offer machine identities, keys or secret services, but scope differs by service. Application-owned accounts and external systems need their own lifecycle and recovery controls.

AIC references: supported platforms · requirements mapping

CQ15 · Capabilities and coverage

Can it manage passwords, SSH keys, certificates, and API keys?

Analog Informatics: Yes. Current capabilities include passwords, SSH keys, certificates and API keys. Verify lifecycle operations against each target-for example issuance, rotation, revocation and dependent application updates-rather than assuming every credential type uses the same mechanism.

FedRAMP cloud services: Providers offer different password, key, certificate and secret services. Check each lifecycle operation and who updates dependent workloads; availability of storage alone is not credential rotation.

AIC references: supported platforms · requirements mapping

CQ16 · Capabilities and coverage

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Does it fix problems automatically, or just tell me they exist?

Analog Informatics: AIC automates discovery, collection, remediation and reporting. Mitigations can run automatically or be surfaced for an administrator to resolve manually. Initial deployment generates a blast-radius report; the administrator can address one finding or all findings at their own pace. Exceptions generate real-time events, including email and text notifications.

FedRAMP cloud services: Provider automation performs the functions included in its service. Customer configuration and workload repair remain customer work unless an explicit managed service takes responsibility for them.

AIC references: supported platforms · requirements mapping

CQ17 · Capabilities and coverage

Does it provide controlled access without exposing credentials?

Analog Informatics: Yes. PAM supplies controlled sessions without disclosing the target credential to the user. PIM can provide approved credential access when that is the required workflow. Test the selected protocol, recording and emergency-access path.

FedRAMP cloud services: Controlled access depends on the chosen provider and customer tools. Trace the actual administrative path, credential disclosure, session evidence and emergency access for the workload being evaluated.

AIC references: supported platforms · requirements mapping

CQ18 · Capabilities and coverage

Can it remove standing privileges and expire approved access automatically?

Analog Informatics: Approved, limited-time access and expiry are part of the privileged-access workflow. Use named people, specified targets, purpose and duration instead of shared standing administration. Test revocation at the target and termination of an already-open session for the chosen protocol.

FedRAMP cloud services: Time-bound roles or approvals may be available in specific services. Verify expiration on the actual workload; a provider role expiring does not establish that every guest-system privilege is removed.

AIC references: supported platforms · requirements mapping

CQ19 · Deployment and customer control

Is it SaaS, self-hosted software, or a managed service?

Analog Informatics: AIC supplies customer-deployed commercial software. The customer or its selected provider operates it. Do not price that as though AIC were also supplying a staffed managed security operation.

FedRAMP cloud services: It can be infrastructure, a platform, an application or another provider-operated service. FedRAMP status does not make all services the same delivery model or define customer software operations.

AIC references: air gapped · security · shared responsibility

CQ20 · Deployment and customer control

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Can I run it on my own hardware or in my own cloud account?

Analog Informatics: Yes. Deploy on customer hardware or supported VMs in the customer's cloud account. The platform documentation distinguishes server hosting from credential-management targets; cloud hosting remains subject to the selected infrastructure and contract requirements.

FedRAMP cloud services: Customers normally consume the provider's defined service. Some products have local variants, but a local installation is not automatically the same authorized service or boundary; establish the exact offering.

AIC references: air gapped · security · shared responsibility

CQ21 · Deployment and customer control

Can it operate in an air-gapped or disconnected environment?

Analog Informatics: Run AIC on premises, in a cloud account you control, in a hybrid environment, or on air-gapped systems for sensitive missions. You choose where the software runs, who administers it and who may use, retrieve or change the secrets it manages. AIC has no standing access to your installation. Air-gapped deployments can be installed, licensed and updated without a network connection to AIC. Design the local identity, time, recovery and approved transfer procedures for that mission. External notifications and integrations need their own permitted communication paths.

FedRAMP cloud services: A provider-connected service cannot be assumed to run as a standalone disconnected installation. For an isolated mission, identify a documented local product and test its operation without external service access.

AIC references: air gapped · security · shared responsibility

CQ22 · Deployment and customer control

Where are my credentials, logs, and compliance evidence stored?

Analog Informatics: Credentials and compliance evidence reside in the customer-deployed environment and its chosen storage/backup architecture. Include replicated logs, exports and backups in the data map. Customer deployment does not automatically determine every external notification or integration destination.

FedRAMP cloud services: The actual service, region, logging configuration, exports and backups determine record locations. Include provider control-plane data and support access rather than examining customer storage alone.

AIC references: air gapped · security · shared responsibility

CQ23 · Deployment and customer control

Who can access my data-including the vendor and its support staff?

Analog Informatics: Access is assigned to customer-authorized roles and delegated operators. Establish named administrators, scoped reviewer access and approval for support sessions. The support-access method depends on the deployment; configure and record it rather than granting standing administrative access by default.

FedRAMP cloud services: The named service's access controls, support process, contracts and personnel arrangements determine provider access. Identify which entities and operators can obtain access and from which locations.

AIC references: air gapped · security · shared responsibility

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ24 · Deployment and customer control

Can I control retention, export my records, and leave without losing evidence?

Analog Informatics: Customers can export credentials, audit logs and compliance evidence in usable formats. Documented evidence outputs include binder PDF and OSCAL. Data can still be exported from an installation after its license expires, although licensed operation stops. Include the required export formats, backups and retention settings in the exit plan.

FedRAMP cloud services: Retention, export and portability are service-specific. Verify usable data, configuration and log exports before changing providers, including the records the customer needs for later assessment and investigation.

AIC references: air gapped · security · shared responsibility

CQ25 · Deployment and customer control

Can my MSP operate it while I retain control?

Analog Informatics: Yes. The customer can select an MSP or qualified provider to operate the software while retaining control of the environment. Give the operator scoped access and retain customer oversight of approvals, records and recovery.

FedRAMP cloud services: An MSP may administer customer accounts through delegated roles. Preserve customer ownership and visibility, and distinguish the MSP’s permissions from access held by the cloud provider itself.

AIC references: air gapped · security · shared responsibility

CQ26 · Deployment and customer control

What happens if the vendor’s service is unavailable?

Analog Informatics: Credential and session services can remain available during Internet or license-service outages in a supported customer-deployed configuration. Local infrastructure and identity dependencies must remain available; external email/text delivery needs a working communication path. A temporary connectivity outage is different from license expiry: operation stops when the license expires, while data export remains available.

FedRAMP cloud services: Provider outages affect dependent infrastructure or applications. Test workload availability, customer identity, independent recovery and evidence access; a service-level credit is not an operational recovery procedure.

AIC references: air gapped · security · shared responsibility

CQ27 · CMMC and continuous compliance

Do I need a full enclave, or will secure email and document sharing be enough?

Analog Informatics: Follow the FCI/CUI data flow. Email/files alone do not address an application, engineering workstation or machine that processes the data outside that boundary. AIC offers customer-deployed enclave and broader privileged-security functions; select the boundary around the actual work.

FedRAMP cloud services: The answer depends on the applications and data flows in scope. A cloud email service does not define the full customer workload boundary, endpoints or privileged administration around it.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

AIC references: supported platforms · requirements mapping

CQ28 · CMMC and continuous compliance

Which CMMC requirements does the software perform, assist with, or document?

Analog Informatics: AIC's requirement-level mapping distinguishes controls the kit performs, activities it assists and evidence it records. Privileged access, credential management, automated collection and remediation operate within the selected package; management decisions and organizational procedures remain assigned to people. Use the level-specific mapping for each assessment objective.

FedRAMP cloud services: Use the exact provider responsibility matrix to identify inherited and customer duties. Then map customer software and procedures to the remaining requirements; the provider's authorization is not the customer's implementation map.

AIC references: supported platforms · requirements mapping

CQ29 · CMMC and continuous compliance

What remains my responsibility or my MSP's responsibility?

Analog Informatics: The customer and chosen MSP handle deployment configuration, FCI/CUI migration, operation, exceptions and organizational practices. Management owns risk decisions. AIC supplies software and its documented capabilities; professional assessment is a separate role.

FedRAMP cloud services: The customer retains duties assigned to it by the service and contract, including workload configuration, account approval, data handling, endpoints and organizational practices unless specifically transferred to a provider.

AIC references: supported platforms · requirements mapping

CQ30 · CMMC and continuous compliance

Does it continuously collect evidence, or will we still gather screenshots before an assessment?

Analog Informatics: Automated collection and reporting are current AIC capabilities. Keep control evidence current as the environment operates. Organizational interviews, policy decisions and physical procedures still need their own records; the goal is to stop reconstructing technical evidence before every review.

FedRAMP cloud services: Provider logs and evidence cover its stated service. Customer workload evidence still needs collection, retention and reviewer access; a provider's compliance package is not every customer operating record.

AIC references: supported platforms · requirements mapping

CQ31 · CMMC and continuous compliance

Can it detect drift and remediate problems between assessments?

Analog Informatics: Yes. Continuous discovery and remediation are the operating model, with real-time exception events and automated reporting. Define the checks, permitted corrections and exception owners for the deployed scope.

FedRAMP cloud services: Some services monitor or remediate configured resources. Define which changes they detect and correct inside customer workloads, and test the handoff for findings that remain customer responsibilities.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

AIC references: supported platforms · requirements mapping

CQ32 · CMMC and continuous compliance

Does it track training, attestations, access approvals, and corrective actions?

Analog Informatics: AIC has training assignments, attestations and attempt records, privileged approval workflows, risk records and corrective evidence. Match package entitlements and the deployed workflow; do not substitute a training record for evidence that a person understood and followed a procedure.

FedRAMP cloud services: These workflows differ across services and customer tools. Identify the system of record for training, attestations, customer approvals and corrective actions instead of assuming the hosting provider supplies them.

AIC references: supported platforms · requirements mapping

CQ33 · CMMC and continuous compliance

Can auditors review current evidence without disrupting IT?

Analog Informatics: AIC provides engagement/evidence workflows and controlled disclosure to reviewers. Prepare scoped access and current reports so IT does not repeat data collection for every request. Auditors still decide what additional evidence they need.

FedRAMP cloud services: Provider compliance documentation and customer evidence have different access paths. Arrange permitted reviewer access to each without sharing administrative credentials or assuming all provider material can be redistributed.

AIC references: supported platforms · requirements mapping

CQ34 · CMMC and continuous compliance

Can it support multiple frameworks without duplicating work?

Analog Informatics: AIC has framework mappings, assessments, control history and evidence records across multiple standards. Reuse a record where its scope and time period support the relevant control; a framework’s presence in a catalog is not equal automation of every requirement.

FedRAMP cloud services: A provider may publish multiple assurance reports. Customer reuse still requires mapping the actual inherited controls and workload evidence to each framework’s scope and requirements.

AIC references: supported platforms · requirements mapping

CQ35 · CMMC and continuous compliance

Can it replace our security-focused GRC tool or feed our existing GRC system?

Analog Informatics: Both approaches are possible. AIC’s own GRC can serve a defined security-compliance scope, while supported exports and event interfaces feed a larger enterprise GRC program. Agree identifiers, fields, retention and ownership before claiming a particular integration is turnkey.

FedRAMP cloud services: A cloud service is not inherently a GRC platform. Retain or add the customer’s required governance and evidence workflow, using supported exports and integrations from the provider and managed systems.

AIC references: supported platforms · requirements mapping

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ36 · Cost and value

What is the total cost-not just the advertised subscription?

Analog Informatics: Total cost includes the selected AIC license, infrastructure, third-party licenses, implementation, operating labor, backups and independent assessment. Published AIC prices remain on the product pricing pages. Compare equal workloads and responsibilities rather than software price against a staffed service.

FedRAMP cloud services: Include infrastructure or application subscriptions, consumption, customer software, integration, operating labor, retention, recovery and assessment work. Compare an equal workload and the same operating responsibilities.

AIC references: pricing · pricing

CQ37 · Cost and value

Is pricing based on users, administrators, identities, systems, or usage?

Analog Informatics: AIC licenses by systems, applications and users, with product-specific package allowances. Counts of human and non-human identities, accounts or credentials do not determine license counts or pricing. Use the current product price list for the applicable meters and entitlements.

FedRAMP cloud services: Licensing can depend on users, compute, storage, transactions, resources or usage. There is no FedRAMP-wide price unit; use the exact service order and workload forecast.

AIC references: pricing · pricing

CQ38 · Cost and value

Are non-human identities charged separately?

Analog Informatics: Human and non-human account counts are not used for AIC license counts or pricing. Passwords, SSH keys, certificates and API keys do not introduce a per-identity charge. Licensed systems, applications and users still determine the selected package and capacity.

FedRAMP cloud services: Identity and machine-access charges depend on the selected service. Count relevant workload identities, secrets, requests and supporting resources where the service’s billing terms require them.

AIC references: pricing · pricing

CQ39 · Cost and value

What costs extra: connectors, reporting, storage, support, or audit access?

Analog Informatics: Enterprise editions and CMMC packages have different allowances for functions and capacity. Free best-effort support is available to all customers; a guaranteed support SLA requires an enterprise support agreement. Infrastructure, third-party software and provider services are separate. Use the current order and price list for exact inclusions.

FedRAMP cloud services: Premium services, support, log retention, connectors, data transfer and recovery can affect the bill. Obtain the selected region’s and service’s actual terms rather than applying another provider’s allowances.

AIC references: pricing · pricing

CQ40 · Cost and value

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

What infrastructure and third-party licenses will I need?

Analog Informatics: Supply supported compute, storage, backup, networking and the operating-system/application licenses the design uses. Customer-cloud deployments incur that provider's charges. Include resilient administration and independent recovery access, not only the minimum server specification.

FedRAMP cloud services: The provider supplies only its contracted service. Customers still supply the operating-system, application and security licenses, network design and software needed for responsibilities outside that service.

AIC references: pricing · pricing

CQ41 · Cost and value

How much staff time does it take to operate?

Analog Informatics: Automation reduces repeated collection, reporting and corrective work, but there is no verified universal staffing figure for an AIC deployment. Measure setup effort and recurring exception/review time in a representative pilot, including the systems automation cannot reach.

FedRAMP cloud services: The provider operates its service; your team operates the customer responsibilities unless another agreement assigns them. Measure customer configuration, exception handling and recovery work rather than counting only provider staff.

AIC references: pricing · pricing

CQ42 · Cost and value

Which manual tasks and existing subscriptions could it eliminate?

Analog Informatics: Candidates include manual credential inventories, repeated rotation work, screenshot collection, evidence assembly and overlapping security/GRC subscriptions. Retire a tool only after its required workflows, records and integrations have been reproduced or deliberately retained elsewhere.

FedRAMP cloud services: Managed infrastructure can remove hosting work. AIC can remove overlapping customer security work. Keep those savings separate and retain any function whose required behavior has not been replaced.

AIC references: pricing · pricing

CQ43 · Cost and value

How do costs change as the company grows?

Analog Informatics: Growth changes licensed systems, applications and users, infrastructure, evidence retention and operating effort. Human and non-human account counts do not drive AIC licensing. Apply the selected package allowances to the forecast and include infrastructure and operating costs.

FedRAMP cloud services: Growth changes the resources, consumption, retention and support the workload needs. Forecast concurrency, data and operating effort, including the cost of maintaining customer controls at the new size.

AIC references: pricing · pricing

CQ44 · Cost and value

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

For hosted VDI, what compute, storage, performance, and usage limits apply?

Analog Informatics: AIC software is not a vendor-hosted VDI seat with a universal CPU/RAM allowance. The customer selects infrastructure capacity. For a marketplace instance or secure-enclave offer, size compute, storage, concurrency, GPU needs and cloud consumption against the actual workload.

FedRAMP cloud services: Only a selected VDI or desktop service has desktop-specific specifications. Obtain its actual compute, storage, graphics, concurrency and usage terms; do not apply a desktop allowance to a generic cloud service.

AIC references: pricing · pricing

CQ45 · Implementation and migration

Can it work with our existing environment, or must we start over?

Analog Informatics: Both. AIC discovers and remediates issues in existing brownfield environments and generates greenfield enclaves. Initial deployment produces a blast-radius report so the administrator can fix one finding or all findings at their own pace. Existing business applications do not all have to move into a new hosted desktop.

FedRAMP cloud services: Compatibility depends on connectivity, identity, supported workloads and the provider’s terms. An AIC pilot can operate alongside existing cloud services when its installation and targets fit the approved design.

AIC references: supported platforms · requirements mapping

CQ46 · Implementation and migration

How quickly can we deploy a new enclave?

Analog Informatics: AIC can generate greenfield enclaves in minutes. That describes enclave generation, not the time to migrate data, integrate every application, train staff or complete an organizational assessment. Scope those subsequent tasks explicitly.

FedRAMP cloud services: Provisioning infrastructure is only one step. Identity, workload hardening, software configuration, data movement, evidence and recovery must be ready before the environment can support the intended work.

AIC references: supported platforms · requirements mapping

CQ47 · Implementation and migration

How long does it take to discover and secure existing systems?

Analog Informatics: No universal time is established for an entire environment. Discovery reachability, account access, dependencies, change windows and the number of exceptions affect the work. Run a measured sample and scale the plan from its findings.

FedRAMP cloud services: Cloud resource discovery and credential protection are different milestones. A successful rotation also requires ownership, dependency updates, verification and recovery for the applications using the credential.

AIC references: supported platforms · requirements mapping

CQ48 · Implementation and migration

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Can we introduce it gradually without interrupting operations?

Analog Informatics: Begin with the initial blast-radius report and choose which findings to address first. Administrators can remediate one finding or all findings at their own pace, using automatic mitigation or manual action. Use change windows, dependency checks and recovery plans to bring an existing environment under control in stages.

FedRAMP cloud services: Yes, when the architecture supports parallel operation and controlled changes. Avoid two independent systems changing the same credential or assuming a migrated workload no longer depends on its old identity service.

AIC references: supported platforms · requirements mapping

CQ49 · Implementation and migration

How do we migrate credentials, policies, and evidence?

Analog Informatics: Inventory credentials and dependencies; map policies; export and preserve historical evidence; pilot import/rotation and reviewer access; then retire old access in stages. Verify export formats and recovery before the change. CMMC data migration belongs to the customer or chosen provider.

FedRAMP cloud services: Export the required workload data, configuration, identities and logs using supported formats. Validate permissions and retention at the destination, and keep a tested rollback before retiring the source service.

AIC references: supported platforms · requirements mapping

CQ50 · Implementation and migration

Who handles configuration, migration, and ongoing operations?

Analog Informatics: The customer or its MSP/qualified provider configures, migrates and operates the environment. AIC supplies commercial software and product guidance. Allocate monitoring, backup, update and exception duties to named owners.

FedRAMP cloud services: The provider configures its service, while the customer or selected operator performs customer responsibilities. Record the boundary in the project plan and responsibility matrix before migration begins.

AIC references: supported platforms · requirements mapping

CQ51 · Implementation and migration

What training, deployment guides, and support are included?

Analog Informatics: All customers receive free best-effort support without a guaranteed SLA. Non-enterprise email support typically responds within 24-72 hours. Purchased enterprise support agreements provide a four-hour response commitment, 24 hours a day, seven days a week; this is a response commitment, not a resolution deadline. Guides, cookbooks, recipes and training materials are included with the products. AIC recommends the customer’s existing MSP or service provider for direct operational support.

FedRAMP cloud services: Training, implementation and support vary by the service and purchased tier. Specify support access, escalation, update responsibilities and procedures for any locally operated or disconnected component.

AIC references: supported platforms · requirements mapping

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ52 · Implementation and migration

Can we test it on our own systems before committing?

Analog Informatics: AIC offers a free 30-day trial of every product. Use the trial to test discovery, controlled access, remediation, evidence exports and exception handling on representative systems. Agree authorized targets and success criteria before connecting production assets.

FedRAMP cloud services: Use an authorized evaluation with representative workloads and permissions. Test access, a failed change, logs, export and recovery; do not infer operational fit solely from an authorization listing.

AIC references: supported platforms · requirements mapping

CQ53 · Vendor credibility and fit

Who supplies and supports this type of environment?

Analog Informatics: Analog Informatics Corporation develops AIC Enterprise Privilege Suite and AIC CMMC Complete. Our cybersecurity experience spans decades. A company founding date is not established in these source materials; discuss the team’s relevant deployment experience and request references for your environment.

FedRAMP cloud services: FedRAMP cloud services are a category, not a single company. Identify the legal provider, service name, applicable boundary and experience with the workload and operating requirements you need.

AIC references: supported platforms · requirements mapping

CQ54 · Vendor credibility and fit

Does it understand organizations like ours?

Analog Informatics: Evaluate AIC against your actual operating problem: shared administration, non-human credentials, brownfield remediation, enclave deployment or current audit evidence. Bring the relevant architecture and constraints to the demonstration; a sector label alone is not proof of fit.

FedRAMP cloud services: Evaluate the specific service’s references and responsibility model for your mission. A general public-sector label does not establish the required application support, administrator access or disconnected behavior.

AIC references: supported platforms · requirements mapping

CQ55 · Vendor credibility and fit

Can it demonstrate our specific use case?

Analog Informatics: Use one real scenario: discover an identity, approve limited access, perform a correction, verify it, then inspect the resulting evidence and exception notification. Include one on-premises and one cloud target where both matter to the purchase.

FedRAMP cloud services: Ask the provider and AIC to demonstrate their respective parts of the same scenario: customer identity, limited administration, a workload correction, resulting evidence and independent recovery.

AIC references: supported platforms · requirements mapping

CQ56 · Vendor credibility and fit

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

What do customers say about reliability and support?

Analog Informatics: No independently verified customer reliability or support measurements are supplied here. Request a customer reference with comparable scale and deployment constraints, and evaluate it alongside the support agreement.

FedRAMP cloud services: Use references and incident history for the exact service and region when available. This category comparison provides no universal reliability or support measurement across all authorized services.

AIC references: supported platforms · requirements mapping

CQ57 · Vendor credibility and fit

What are its limitations?

Analog Informatics: Product/package coverage, supported targets and operational dependencies define the boundary. Broad SaaS connector parity, universal bidirectional GRC integration, a full LMS and every financial-risk function have not been established. Customer control does not eliminate licensing, backup or operating obligations.

FedRAMP cloud services: The authorization boundary, supported services, access terms and customer duties define the limitations. Features from another product or region should not be assumed to belong to the selected offering.

AIC references: supported platforms · requirements mapping

CQ58 · Vendor credibility and fit

Which capabilities are available today, and which are roadmap items?

Analog Informatics: Use the released functions and entitlements of the selected AIC product and CMMC level for a purchase today. AIC’s broader platform includes PIM, PAM, PUM, IGA, GRC, CLM and CIAM. Competing features remain within future development scope without a commitment to a particular feature or release date.

FedRAMP cloud services: Only the released functions and terms of the exact service are available today. Planned regions, authorization changes and proposed features remain future items until the provider makes them available.

AIC references: supported platforms · requirements mapping

CQ59 · Vendor credibility and fit

How does it handle vulnerabilities and security updates?

Analog Informatics: Vulnerability notification considers severity, likelihood, impact and which customers may be affected. AIC generally responds within 24 hours to a severe vulnerability report and typically has a mitigation within 24 hours of notice. These are typical best-effort practices, not guaranteed mitigation deadlines; the specific issue determines the work required. Customers and their providers incorporate mitigations and updates into their controlled operating process, including offline deployments.

FedRAMP cloud services: The provider handles service-side vulnerabilities under its process; customers handle their assigned workload updates. Coordinate advisories, testing and recovery, including offline components that cannot receive automatic updates.

AIC references: security

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ60 · Vendor credibility and fit

Will it work with our existing vendors and service providers?

Analog Informatics: AIC works alongside Microsoft, existing infrastructure, MSPs and external GRC using supported integrations and exports. Agree the version, fields, permissions and operating responsibilities for each connection.

FedRAMP cloud services: Compatibility is integration- and contract-specific. Trace identities, permissions, network paths, logs and support ownership across your selected providers rather than assuming all products from one company are integrated.

AIC references: supported platforms · requirements mapping

CQ61 · Vendor credibility and fit

What happens to our deployment if the vendor is acquired or changes direction?

Analog Informatics: Customers retain control of their deployed environment, credentials and evidence. AIC software stops operating when its license expires, but data can still be exported from the expired installation. Customer deployment does not mean perpetual licensed operation. Maintain tested backups and independent emergency access, and include exports in the exit plan.

FedRAMP cloud services: Provider acquisition or contract changes can affect service continuity and access. Preserve usable exports, customer-owned records and a tested transition plan; negotiate any continuity rights the mission requires.

AIC references: supported platforms · requirements mapping

Sources and scope

Deployment and customer-control statements reflect the product owner’s November 20, 2026 instructions and AIC’s documented deployment model. The alternative is a category rather than one standardized product or contract. Specific unverified service terms and implementation details are identified in the answers.

- https://analoginfo.com/supported-platforms
- https://analoginfo.com/cmmc/pricing
- https://analoginfo.com/cmmc/requirements-mapping
- https://analoginfo.com/security
- https://analoginfo.com/air-gapped
- https://analoginfo.com/shared-responsibility
- https://analoginfo.com/cmmc/compare/microsoft-gcc-high
- https://analoginfo.com/cmmc/compare/aws-govcloud

© 2026 Analog Informatics Corporation. For more information about Analog Informatics Corporation, please go to analoginfo.com.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.