COMPETITIVE ANALYSIS

Analog Informatics vs. Managed CMMC Services - Competitive Analysis

Choose who runs CMMC operations: your team with AIC or a managed provider. Compare staff duties, secret access, evidence custody and isolated mission support.

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 lets the customer keep ownership of its installation, secret-access rules and evidence while choosing its own operators. An MSP can use the same platform under customer-approved roles instead of requiring the customer to surrender its operating records to a particular service bundle.

Suitable customers: Organizations with an internal operating team, a preferred MSP, country-specific administration requirements or a sensitive disconnected mission that needs local authority over secrets and records.

Where the alternative fits

An appropriate managed provider can supply implementation expertise, recurring administration and defined support coverage. That is valuable when the customer lacks the staff or capacity to run the environment and wants accountable operating duties under contract.

Suitable customers: Customers that need ongoing staff to configure, monitor and maintain the agreed environment. A provider can operate AIC when the service scope and customer-control 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.

managed CMMC services: It is a service relationship whose tool hosting can be local, cloud or mixed. Separate the location of the software from the location and authority of the people operating it.

Customer hardware or cloud account

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

managed CMMC services: Some providers operate customer-owned infrastructure and others require their own hosted environment. The contract should state ownership, administrator rights, export access and the terms for continuing software use.

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.

managed CMMC services: Local service work is possible only when the provider’s people and tools can meet the disconnected design. Demonstrate identity, maintenance, updates, evidence access and incident response without an assumed remote connection.

Secret and evidence custody

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

managed CMMC services: Records may reside in customer systems, provider platforms or both. Identify credential storage, session recordings, ticket data, compliance evidence, backups and the customer’s independent access to each.

Support and operator access

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

managed CMMC services: Named customer and provider roles, subcontractors and support arrangements determine access. Establish operator identity, location, approval, logging and removal procedures for the sensitive systems and secrets in scope.

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.

managed CMMC 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.

managed CMMC services: A provider change can affect people, access and bundled software rights. Retain customer-owned credentials and records, tested exports, independent emergency access and a transition plan for reassigned operating duties.

CQ01 · Alternatives and switching

What are the best alternatives to managed CMMC 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.

managed CMMC services: Alternatives include operating AIC with your own team, selecting an MSP to operate AIC or choosing another managed service. The right option depends on the duties and coverage you need.

AIC references: supported platforms · requirements mapping

CQ02 · Alternatives and switching

Which companies compete with managed CMMC 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.

managed CMMC services: Managed CMMC services come from multiple providers, including specialist compliance and security firms. Compare the named legal supplier, service scope and tool rights rather than treating the category as one product.

AIC references: supported platforms · requirements mapping

CQ03 · Alternatives and switching

How does AIC compare with managed CMMC services?

Analog Informatics: Compare the AIC software purchase with the software portion of the managed proposal, then compare who will perform the remaining service work. 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.

managed CMMC services: AIC supplies customer-operated software. A managed provider supplies the people and contracted duties in its proposal, often with several tools. The provider can also operate AIC under an agreed customer-control model.

AIC references: supported platforms · requirements mapping

CQ04 · Alternatives and switching

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Can AIC replace managed CMMC 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.

managed CMMC services: You may need both. AIC can replace overlapping software while the provider continues implementation, monitoring, remediation or support tasks. Do not retire staffed duties without assigning them to someone else.

AIC references: supported platforms · requirements mapping

CQ05 · Alternatives and switching

Why would I switch from managed CMMC 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.

managed CMMC services: Change when the current service's access model, evidence ownership, response coverage or responsibilities no longer fit. Keep useful people and tools when a different platform would not improve the operating result.

AIC references: supported platforms · requirements mapping

CQ06 · Alternatives and switching

Is there a self-hosted alternative to managed CMMC 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.

managed CMMC services: AIC is an installable option for the software layer. A managed provider may operate customer-hosted systems too; establish who owns the installation and which software rights remain when the service ends.

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.

managed CMMC services: A provider may bundle several tools and AIC may consolidate overlapping functions. Identify each required task and evidence record before removing an underlying product from the service.

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.

managed CMMC services: Taking work in-house can increase direct control but adds operating duties. A new provider may offer better coverage while changing tools or access paths. Preserve required records and recovery throughout the transition.

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.

managed CMMC services: The answer is the contracted scope. Determine whether the provider covers the full workload, only an enclave or selected compliance tasks, and identify responsibilities left to customer staff.

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.

managed CMMC services: Included software, administration, monitoring, assessment preparation and support differ by provider. Use the actual statement of work and entitlements; a package name does not establish every required function.

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.

managed CMMC services: A provider may manage on-premises and cloud systems, but the supported boundary is contract-specific. Include factory systems, local applications, remote users and exceptions in the proposed scope.

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.

managed CMMC services: Coverage depends on the provider's tools, expertise and service terms. Demonstrate the actual operations on representative Windows, Linux, network and older systems, including targets outside the standard managed image.

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.

managed CMMC services: Only if the provider's tools and operating scope include discovery. Review the inventory and unresolved ownership or dependency findings; managed service enrollment alone does not prove credential coverage.

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.

managed CMMC services: Define the service's responsibility for service accounts, application identities and AI credentials. Identify who can discover, rotate, approve and recover each identity, and which supporting tools perform the work.

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.

managed CMMC services: The proposal must identify lifecycle support for each credential type. Vault storage, certificate issuance, key rotation and updates to dependent services can be performed by different products and operators.

AIC references: supported platforms · requirements mapping

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ16 · Capabilities and coverage

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.

managed CMMC services: The provider may use automation, manual response or both. Specify who approves and performs corrections, response coverage and how successful repair is verified in the customer's evidence record.

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.

managed CMMC services: Access without credential disclosure depends on the provider's actual remote-access and vault design. Demonstrate a customer-approved session, recording, emergency path and the permissions granted to provider personnel.

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.

managed CMMC services: The selected tools and operating policy determine temporary access. Test approval, expiration and revocation for provider operators as well as customer administrators, including access after a technician changes roles.

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.

managed CMMC services: It is a service relationship whose tool hosting can be local, cloud or mixed. Separate the location of the software from the location and authority of the people operating it.

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.

managed CMMC services: Some providers operate customer-owned infrastructure and others require their own hosted environment. The contract should state ownership, administrator rights, export access and the terms for continuing software use.

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.

managed CMMC services: Local service work is possible only when the provider's people and tools can meet the disconnected design. Demonstrate identity, maintenance, updates, evidence access and incident response without an assumed remote connection.

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.

managed CMMC services: Records may reside in customer systems, provider platforms or both. Identify credential storage, session recordings, ticket data, compliance evidence, backups and the customer's independent access to each.

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.

managed CMMC services: Named customer and provider roles, subcontractors and support arrangements determine access. Establish operator identity, location, approval, logging and removal procedures for the sensitive systems and secrets in scope.

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.

managed CMMC services: The service contract and technical design determine retention, export and exit support. Obtain independently readable records and verify customer access before terminating the agreement or changing providers.

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.

managed CMMC services: Yes, if the design preserves customer ownership and oversight. Give the MSP scoped access, retain customer administration and emergency recovery, and make evidence export part of normal operation.

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.

managed CMMC services: Provider outages or staffing failures affect the duties assigned to it. Define incident coverage, customer emergency operation, alternate contacts and access to records without depending on one provider account.

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.

managed CMMC services: The service must match the customer’s actual FCI/CUI work. Email and files may be insufficient when the job also uses local applications, engineering systems, external devices or privileged maintenance.

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.

managed CMMC services: Use the provider's responsibility matrix and the selected software's requirement mapping. Distinguish technical operation, evidence assistance and customer organizational duties rather than assuming the service performs everything.

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.

managed CMMC services: Your organization retains duties not expressly assigned elsewhere, including business decisions, policy ownership and customer actions. A provider's work still needs customer oversight and clear accountability for exceptions.

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.

managed CMMC services: Specify which evidence is collected automatically and which records staff maintain. Review currency and failed collection between assessments, including whether the customer can access the underlying operating records.

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.

managed CMMC services: Some providers monitor drift and perform agreed corrections. Define the covered systems, authority to change them, response process and verification, including findings the provider must escalate to the customer.

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.

managed CMMC services: The service may deliver these workflows through separate tools and staff. Assign an owner and system of record for training versions, attestations, access approvals and corrective actions.

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.

managed CMMC services: Auditor access and evidence handling must be agreed with the provider and customer. Scoped reviewer access or retained exports can reduce disruption without granting the assessor broad administrative access.

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.

managed CMMC services: A provider can support multiple frameworks when its methods and tools cover them. Reuse shared evidence while keeping framework-specific scope and duties clear; confirm the actual contract includes the required work.

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.

managed CMMC services: Some providers include a GRC platform; others provide services around the customer’s tools. Establish which records, integrations and software rights the customer retains if the service or provider changes.

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.

managed CMMC services: Include onboarding, service fees, required software, infrastructure, support options, retained customer labor and independent assessment. Compare the same operating boundary and service coverage before deciding which option costs less.

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.

managed CMMC services: Providers may charge by users, systems, locations, workload or an agreed service scope. There is no universal managed-CMMC price unit; obtain the exact meters, minimums and growth terms.

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.

managed CMMC services: Service-account or machine-identity treatment varies by provider and included tools. Document any identity, system, credential or usage charges in the proposal rather than assuming employee seats cover 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.

managed CMMC services: Project work, special integrations, storage, after-hours response, premium support and assessment participation may be separate. Distinguish recurring service inclusions from work that needs another authorization or fee.

AIC references: pricing · pricing

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

CQ40 · Cost and value

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.

managed CMMC services: The provider may include infrastructure and licenses or require the customer to supply them. Identify every component, account owner and renewal responsibility, including recovery and retention systems.

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.

managed CMMC services: The provider performs agreed duties, but customer coordination, approvals and exceptions remain. Measure both parties' routine workload and escalation effort; no category-wide customer staffing figure applies.

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.

managed CMMC services: Managed operation can remove tasks the service actually takes over. Verify the changed workflow, record ownership and response coverage before eliminating internal capacity or another subscription.

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.

managed CMMC services: Growth can change service tiers, license counts, supported systems, locations, evidence retention and staffing. Model those changes with the provider's actual pricing and capacity terms.

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.

managed CMMC services: Only a proposal that includes VDI defines desktop allowances. Obtain actual compute, storage, graphics, concurrent use, application performance and consumption terms, rather than assuming a standard managed desktop fits the workload.

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.

managed CMMC services: Some services integrate existing systems and others require a standard environment. Inventory applications, data, devices and controls the provider will retain, migrate or exclude before agreeing to the transition.

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.

managed CMMC services: Time depends on the provider’s delivery scope, customer readiness, data movement and control work. Establish acceptance criteria for a working environment and evidence, not just account provisioning.

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.

managed CMMC services: The service must distinguish inventory from verified protection. A discovered account still needs an owner, dependency review, controlled change and evidence that its dependent work continues successfully.

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.

managed CMMC services: A staged introduction can work when both teams agree authority and recovery. Avoid overlapping change schedules and keep the current provider's necessary duties covered until the new arrangement is accepted.

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.

managed CMMC services: Define the supported exports and imports for credentials, policies, records and tickets. Verify the destination's access and evidence quality, retain independent copies and agree a rollback before cutover.

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.

managed CMMC services: The statement of work assigns configuration, migration and recurring operation. Record customer prerequisites and provider duties explicitly; buying a platform or service does not complete that responsibility assignment.

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.

managed CMMC services: Training, deployment documentation and support depend on the agreement and tools. Specify named escalation, coverage hours, supported changes, isolated-site procedures and who retains documentation when staff change.

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.

managed CMMC services: Ask for an agreed pilot on representative systems. Test a failed change, approved access, evidence export and recovery, with acceptance criteria and responsibilities for both parties.

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.

managed CMMC services: This category has no single company history. Assess the actual legal provider, relevant staff, subcontractors, customer references and continuity plan for the service it proposes to deliver.

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.

managed CMMC services: Look for experience with your applications, data boundary, staffing and administration constraints. A broad defense or compliance label does not establish that the provider can operate your specific mission.

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.

managed CMMC services: Use a customer-representative exercise with the proposed technicians and tools: approved access, a credential change, a failed repair, escalation, evidence review and emergency operation.

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.

managed CMMC services: Request references and incident history for a comparable service and customer environment. This comparison provides no independent category-wide reliability or support measurement and invents no customer testimonial.

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.

managed CMMC services: The service boundary, staffing coverage, selected tools and change authority are the limits. Identify exclusions and dependencies, including systems or locations that require customer staff or another supplier.

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.

managed CMMC services: Count only released tools and services included in the signed scope. A proposed integration, future staffing service or vendor roadmap item is not a current delivered capability.

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.

managed CMMC services: The agreement should assign advisory review, change approval, patch deployment, verification and recovery. Include the offline transfer process and the customer/provider handoff for systems outside the standard service.

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.

managed CMMC services: Compatibility depends on permitted integrations, customer contracts and cooperation between operators. Agree who owns tickets, credentials, evidence and escalation across existing vendors before assigning ongoing work.

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.

managed CMMC services: A provider change can affect people, access and bundled software rights. Retain customer-owned credentials and records, tested exports, independent emergency access and a transition plan for reassigned operating duties.

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/summit-7
- https://analoginfo.com/cmmc/compare/cybersheath
- https://analoginfo.com/cmmc/compare/ardalyst

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.