COMPETITIVE ANALYSIS

Analog Informatics vs. Vanta, Drata and Secureframe - Competitive Analysis

Compare AIC with Vanta, Drata and Secureframe: operational controls, compliance workflows, evidence custody and customer-operated or air-gapped deployment.

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 connects credential changes, approved administration and configuration work to operating evidence. Customers can place and manage the software where their mission requires, including disconnected systems, and choose who can access managed secrets and records.

Suitable customers: Security and IT teams that need to perform privileged controls and corrective work, retain local custody of secrets and evidence, or operate a mission that cannot depend on an external compliance service.

Where the alternative fits

The three platforms emphasize compliance programs, connected evidence and workflow coordination. Their specific integrations, program functions and support differ; the detailed answers below retain the supplier-specific findings from each published analysis.

Suitable customers: Teams whose main purchase is a connected compliance program and its supported workflows. Keep a useful program when it still performs necessary work, and evaluate AIC alongside it for the operating controls.

Evaluate each compliance platform separately

Vanta

Vanta organizes CMMC workflows, automates connected evidence collection, monitors controls and maps framework requirements. It fits a team whose main purchase is keeping a connected compliance program current.

Drata

Drata emphasizes CMMC controls, continuous evidence and defined ownership across compliance programs. It fits teams coordinating control owners and recurring evidence from supported connections.

Secureframe

Secureframe provides cloud compliance workflows and Defense Navigator provisioning in the customer’s Azure Government environment. It fits teams evaluating that combination of SSP work and a customer-owned cloud enclave. The enclave and the vendor-operated compliance platform remain separate parts of the design.

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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

Deployment comparison

Management service

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

Vanta: Vendor-hosted SaaS compliance software with connected evidence and workflow functions.

Drata: Vendor-hosted SaaS compliance software with control ownership, evidence and program functions.

Secureframe: Vendor-hosted compliance software, with Defense Navigator provisioning a separate enclave in the customer’s Azure Government environment.

Customer hardware or cloud account

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

Vanta: The published material reviewed for Vanta does not specify a customer-hardware or customer-account deployment of the entire named offering. Ask which components remain vendor-hosted and which may run in your account; a local connector does not make the whole service self-hosted.

Drata: The published material reviewed for Drata does not specify a customer-hardware or customer-account deployment of the entire named offering. Ask which components remain vendor-hosted and which may run in your account; a local connector does not make the whole service self-hosted.

Secureframe: Secureframe provides cloud compliance workflows and Defense Navigator provisioning in the customer’s Azure Government environment. The customer-hosted enclave is distinct from the compliance platform. The customer still needs the documented infrastructure, license and operating skills.

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Vanta: The published material reviewed for Vanta does not specify fully disconnected operation, including license validation, authentication and updates. Require an offline test rather than infer air-gap support from self-hosting or a local agent. Document which functions stop when external connectivity is removed.

Drata: The published material reviewed for Drata does not specify fully disconnected operation, including license validation, authentication and updates. Require an offline test rather than infer air-gap support from self-hosting or a local agent. Document which functions stop when external connectivity is removed.

Secureframe: The published material reviewed for Secureframe does not specify fully disconnected operation, including license validation, authentication and updates. Require an offline test rather than infer air-gap support from self-hosting or a local agent. Document which functions stop when external connectivity is removed.

Secret and evidence custody

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

Vanta: The offering reviewed is a cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places. The reviewed architecture does not fully resolve storage/replication locations for credentials, evidence, logs and backups. Obtain the data-flow and hosting schedule for the exact edition, including subprocessors and optional integrations.

Drata: The offering reviewed is a cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places. The reviewed architecture does not fully resolve storage/replication locations for credentials, evidence, logs and backups. Obtain the data-flow and hosting schedule for the exact edition, including subprocessors and optional integrations.

Secureframe: Secureframe provides cloud compliance workflows and Defense Navigator provisioning in the customer’s Azure Government environment. The customer-hosted enclave is distinct from the compliance platform. The reviewed architecture does not fully resolve storage/replication locations for credentials, evidence, logs and backups. Obtain the data-flow and hosting schedule for the exact edition, including subprocessors and optional integrations.

Support and operator access

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

Vanta: The published material reviewed for Vanta does not specify the exact supplier-support access, key custody and privileged access approval controls for the proposed tenant. Request the access model and contractual commitments, including support elevation, audit records and subprocessors. SaaS does not by itself mean the customer has no data control.

Drata: The published material reviewed for Drata does not specify the exact supplier-support access, key custody and privileged access approval controls for the proposed tenant. Request the access model and contractual commitments, including support elevation, audit records and subprocessors. SaaS does not by itself mean the customer has no data control.

Secureframe: The published material reviewed for Secureframe does not specify the exact supplier-support access, key custody and privileged access approval controls for the proposed tenant. Request the access model

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

and contractual commitments, including support elevation, audit records and subprocessors. SaaS does not by itself mean the customer has no data control.

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.

Vanta: Confirm the Vanta service location, subprocessors, administrator access, support locations and retained record copies; no local installation of the complete named service is established in the reviewed material.

Drata: Confirm the Drata service location, subprocessors, administrator access, support locations and retained record copies; no local installation of the complete named service is established in the reviewed material.

Secureframe: Evaluate the customer's Azure Government enclave separately from the vendor-operated compliance platform. Include both components, support access and record copies in the location review.

Provider independence

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

Vanta: An acquisition or strategy change does not by itself determine your rights. The reviewed Vanta material does not establish a perpetual right to use all components or a complete exit guarantee. Retain the current agreement, renewal/termination provisions, exports and a tested continuity plan.

Drata: An acquisition or strategy change does not by itself determine your rights. The reviewed Drata material does not establish a perpetual right to use all components or a complete exit guarantee. Retain the current agreement, renewal/termination provisions, exports and a tested continuity plan.

Secureframe: An acquisition or strategy change does not by itself determine your rights. The reviewed Secureframe material does not establish a perpetual right to use all components or a complete exit guarantee. Retain the current agreement, renewal/termination provisions, exports and a tested continuity plan.

CQ01 · Alternatives and switching

What are the best alternatives to Vanta, Drata and Secureframe?

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.

Vanta: For the GRC and audit software portion of the purchase, shortlist Drata, Secureframe, Thoropass, Sprinto. AIC is the customer-deployed security/control option. The best fit depends on whether you need software, operating staff, collaboration or governance; compare that job before ranking vendors.

Drata: For the GRC and audit software portion of the purchase, shortlist Vanta, Secureframe, Thoropass, Sprinto. AIC is the customer-deployed security/control option. The best fit depends on whether you need software, operating staff, collaboration or governance; compare that job before ranking vendors.

Secureframe: For the GRC and audit software portion of the purchase, shortlist Vanta, Drata, Thoropass, Sprinto. AIC is the customer-deployed security/control option. The best fit depends on whether you need software, operating staff, collaboration or governance; compare that job before ranking vendors.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

AIC references: supported platforms · requirements mapping

CQ02 · Alternatives and switching

Which companies compete with Vanta, Drata and Secureframe?

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.

Vanta: Drata, Secureframe, Thoropass, Sprinto are adjacent offerings in this comparison set. They overlap in different ways with Vanta; they are not identical replacements. AIC overlaps where privileged controls, remediation and security evidence are the required outcome.

Drata: Vanta, Secureframe, Thoropass, Sprinto are adjacent offerings in this comparison set. They overlap in different ways with Drata; they are not identical replacements. AIC overlaps where privileged controls, remediation and security evidence are the required outcome.

Secureframe: Vanta, Drata, Thoropass, Sprinto are adjacent offerings in this comparison set. They overlap in different ways with Secureframe; they are not identical replacements. AIC overlaps where privileged controls, remediation and security evidence are the required outcome.

AIC references: supported platforms · requirements mapping

CQ03 · Alternatives and switching

How does AIC compare with Vanta, Drata and Secureframe?

Analog Informatics: For this decision, separate the compliance program from the system that performs the privileged change or repair. 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.

Vanta: Vanta emphasizes CMMC workflows, evidence automation, control monitoring and framework mapping. Compare this with AIC’s customer-deployed operating controls and the required evidence flow. The specific purchasing difference is: Connect credential rotation, approved sessions and verified repairs to the control record.

Drata: Drata emphasizes CMMC controls, continuous evidence and defined ownership across compliance programs. Compare this with AIC’s customer-deployed operating controls and the required evidence flow. The specific purchasing difference is: Generate access, session and configuration evidence from the security controls themselves.

Secureframe: Secureframe emphasizes Defense Navigator, SSP workflows and automated CUI enclave configuration in customer-owned cloud environments. Compare this with AIC’s customer-deployed operating controls and the required evidence flow. The specific purchasing difference is: Compare customer-deployed credential, session, configuration and evidence functions across the actual systems in scope.

AIC references: supported platforms · requirements mapping

CQ04 · Alternatives and switching

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Can AIC replace Vanta, Drata and Secureframe, 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.

Vanta: Retain useful SaaS integrations and trust workflows; compare overlapping audit and evidence functions before retiring them.

Drata: Keep enterprise-wide compliance programs in Drata where they serve broader obligations; supply operational evidence through an agreed interface.

Secureframe: Evaluate Defense enclave provisioning separately from compliance workflows. Secureframe is not merely a document checklist.

AIC references: supported platforms · requirements mapping

CQ05 · Alternatives and switching

Why would I switch from Vanta, Drata and Secureframe?

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.

Vanta: Your evidence is collected, but privileged changes still happen outside the compliance workflow. A change is justified when the pilot resolves that problem and the transition preserves required functions.

Drata: Teams answer the same control question in several systems while administrators work in another. A change is justified when the pilot resolves that problem and the transition preserves required functions.

Secureframe: A cloud enclave may cover the office workflow while factory systems and privileged accounts still need controls. A change is justified when the pilot resolves that problem and the transition preserves required functions.

AIC references: supported platforms · requirements mapping

CQ06 · Alternatives and switching

Is there a self-hosted alternative to Vanta, Drata and Secureframe?

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.

Vanta: AIC is a self-hosted option for the overlapping security work. The offering reviewed is a cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places. A self-hosted edition of this exact offering has not been established in the material reviewed; request a written deployment architecture if that is mandatory.

Drata: AIC is a self-hosted option for the overlapping security work. The offering reviewed is a cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places. A self-hosted edition of this exact offering has not been established in the material reviewed; request a written deployment architecture if that is mandatory.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Secureframe: AIC is a self-hosted option for the overlapping security work. Secureframe provides cloud compliance workflows and Defense Navigator provisioning in the customer's Azure Government environment. The customer-hosted enclave is distinct from the compliance platform. A self-hosted edition of this exact offering has not been established in the material reviewed; request a written deployment architecture if that is mandatory.

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.

Vanta: The published scope combines CMMC workflows, evidence automation, control monitoring and framework mapping. Whether that eliminates other tools depends on retained connectors, controls and service duties. Build a function-by-function retirement list rather than assume an entire stack is replaced.

Drata: The published scope combines CMMC controls, continuous evidence and defined ownership across compliance programs. Whether that eliminates other tools depends on retained connectors, controls and service duties. Build a function-by-function retirement list rather than assume an entire stack is replaced.

Secureframe: The published scope combines Defense Navigator, SSP workflows and automated CUI enclave configuration in customer-owned cloud environments. Whether that eliminates other tools depends on retained connectors, controls and service duties. Build a function-by-function retirement list rather than assume an entire stack is replaced.

AIC references: supported platforms · requirements mapping

CQ08 · Alternatives and switching

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.

Vanta: The functions to preserve are CMMC workflows, evidence automation, control monitoring and framework mapping. The potential gain from AIC is customer-operated control and evidence in the same workflow. Export control mappings, evidence history and owner assignments; prove that the replacement preserves required audit workflows.

Drata: The functions to preserve are CMMC controls, continuous evidence and defined ownership across compliance programs. The potential gain from AIC is customer-operated control and evidence in the same workflow. Map shared controls and evidence retention first, then pilot one scope before changing the compliance system of record.

Secureframe: The functions to preserve are Defense Navigator, SSP workflows and automated CUI enclave configuration in customer-owned cloud environments. The potential gain from AIC is customer-operated control and evidence in the same workflow. Preserve the cloud boundary and SSP, then test supported operating systems, administrative paths and evidence exports before changing platforms.

AIC references: supported platforms · requirements mapping

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Vanta: This is a cloud compliance platform, so evaluate it for that role. The stated product scope does not establish that it covers every organizational duty, infrastructure dependency and application in your environment.

Drata: This is a cloud compliance platform, so evaluate it for that role. The stated product scope does not establish that it covers every organizational duty, infrastructure dependency and application in your environment.

Secureframe: This is Compliance platform with customer-cloud enclave provisioning, so evaluate it for that role. The stated product scope does not establish that it covers every organizational duty, infrastructure dependency and application in your environment.

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.

Vanta: The published capability summary is CMMC workflows, evidence automation, control monitoring and framework mapping. Exact entitlements, optional modules and third-party dependencies require the selected package’s bill of materials. Preserve the distinction between product features and separately purchased professional services.

Drata: The published capability summary is CMMC controls, continuous evidence and defined ownership across compliance programs. Exact entitlements, optional modules and third-party dependencies require the selected package’s bill of materials. Preserve the distinction between product features and separately purchased professional services.

Secureframe: The published capability summary is Defense Navigator, SSP workflows and automated CUI enclave configuration in customer-owned cloud environments. Exact entitlements, optional modules and third-party dependencies require the selected package’s bill of materials. Preserve the distinction between product features and separately purchased professional services.

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Vanta: The published material reviewed for Vanta does not specify the exact on-premises/cloud target inventory and operations for each target. Obtain the connector/protocol matrix and test one local and one cloud workload. Hosting location alone does not answer managed-asset coverage.

Drata: The published material reviewed for Drata does not specify the exact on-premises/cloud target inventory and operations for each target. Obtain the connector/protocol matrix and test one local and one cloud workload. Hosting location alone does not answer managed-asset coverage.

Secureframe: Defense Navigator configures customer-owned cloud environments; Federal MDM covers customer endpoints. Compare those functions with privileged credential and session management across the wider environment.

AIC references: supported platforms · requirements mapping

CQ12 · Capabilities and coverage

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.

Vanta: The published material reviewed for Vanta does not specify an exhaustive Windows/Linux/network-device/legacy support matrix for the required functions. Separate endpoints that can access the service from systems whose credentials or configurations it can actually manage. Request versions, protocols and extension limits.

Drata: The published material reviewed for Drata does not specify an exhaustive Windows/Linux/network-device/legacy support matrix for the required functions. Separate endpoints that can access the service from systems whose credentials or configurations it can actually manage. Request versions, protocols and extension limits.

Secureframe: Federal MDM lists Windows, macOS and Linux. Network-device and legacy credential-management coverage is not specified in the cited setup guide; evaluate those targets separately.

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.

Vanta: The published material reviewed for Vanta does not specify discovery of previously unknown privileged credentials, rather than asset inventory or integration-fed evidence. Ask for a discovery run that produces a new account, its owner and target dependency, not only a compliance dashboard.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: The published material reviewed for Drata does not specify discovery of previously unknown privileged credentials, rather than asset inventory or integration-fed evidence. Ask for a discovery run that produces a new account, its owner and target dependency, not only a compliance dashboard.

Secureframe: The published material reviewed for Secureframe does not specify discovery of previously unknown privileged credentials, rather than asset inventory or integration-fed evidence. Ask for a discovery run that produces a new account, its owner and target dependency, not only a compliance dashboard.

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.

Vanta: The published material reviewed for Vanta does not specify the complete lifecycle of service accounts and AI-agent identities. Identify the underlying identity, target application, discovery method and rotation/revocation operation, then test that chain.

Drata: The published material reviewed for Drata does not specify the complete lifecycle of service accounts and AI-agent identities. Identify the underlying identity, target application, discovery method and rotation/revocation operation, then test that chain.

Secureframe: The published material reviewed for Secureframe does not specify the complete lifecycle of service accounts and AI-agent identities. Identify the underlying identity, target application, discovery method and rotation/revocation operation, then test that chain.

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.

Vanta: The published material reviewed for Vanta does not specify full discover/rotate/revoke/propagate coverage for passwords, SSH keys, certificates and API keys. Use a four-type credential test plan. Storing a secret is not equivalent to rotating it on the target or updating dependent services.

Drata: The published material reviewed for Drata does not specify full discover/rotate/revoke/propagate coverage for passwords, SSH keys, certificates and API keys. Use a four-type credential test plan. Storing a secret is not equivalent to rotating it on the target or updating dependent services.

Secureframe: The published material reviewed for Secureframe does not specify full discover/rotate/revoke/propagate coverage for passwords, SSH keys, certificates and API keys. Use a four-type credential test plan. Storing a secret is not equivalent to rotating it on the target or updating dependent services.

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.

Vanta: The published material reviewed for Vanta does not specify which corrective actions execute directly on the customer's target systems. Demonstrate one failed check through authorization, actual correction, verification and evidence; distinguish an assigned ticket from an executed repair.

Drata: Drata describes control testing, linked evidence, ownership and POA&M oversight. Those workflows do not establish which changes it executes on your specific hosts; require an actual failing-control repair demonstration.

Secureframe: Navigator applies supported enclave configurations automatically, validates them with tests and flags drift. Compare initial configuration with the corrective actions available after deployment.

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.

Vanta: The published material reviewed for Vanta does not specify credential-hidden privileged sessions to the customer's target systems. Demonstrate the administrative connection, not only single sign-on to a collaboration or GRC portal. Identify any additional PAM product required.

Drata: The published material reviewed for Drata does not specify credential-hidden privileged sessions to the customer's target systems. Demonstrate the administrative connection, not only single sign-on to a collaboration or GRC portal. Identify any additional PAM product required.

Secureframe: The published material reviewed for Secureframe does not specify credential-hidden privileged sessions to the customer's target systems. Demonstrate the administrative connection, not only single sign-on to a collaboration or GRC portal. Identify any additional PAM product required.

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.

Vanta: The published material reviewed for Vanta does not specify end-to-end grant expiry, target revocation and already-open session termination for the chosen workload. Test a named, time-bounded approval and observe what actually stops at expiry. Role activation alone does not prove every target session is terminated.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: The published material reviewed for Drata does not specify end-to-end grant expiry, target revocation and already-open session termination for the chosen workload. Test a named, time-bounded approval and observe what actually stops at expiry. Role activation alone does not prove every target session is terminated.

Secureframe: The published material reviewed for Secureframe does not specify end-to-end grant expiry, target revocation and already-open session termination for the chosen workload. Test a named, time-bounded approval and observe what actually stops at expiry. Role activation alone does not prove every target session is terminated.

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.

Vanta: The offering reviewed is a cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places.

Drata: The offering reviewed is a cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places.

Secureframe: Secureframe provides cloud compliance workflows and Defense Navigator provisioning in the customer’s Azure Government environment. The customer-hosted enclave is distinct from the compliance platform.

AIC references: air gapped · security · shared responsibility

CQ20 · Deployment and customer control

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.

Vanta: The published material reviewed for Vanta does not specify a customer-hardware or customer-account deployment of the entire named offering. Ask which components remain vendor-hosted and which may run in your account; a local connector does not make the whole service self-hosted.

Drata: The published material reviewed for Drata does not specify a customer-hardware or customer-account deployment of the entire named offering. Ask which components remain vendor-hosted and which may run in your account; a local connector does not make the whole service self-hosted.

Secureframe: Secureframe provides cloud compliance workflows and Defense Navigator provisioning in the customer’s Azure Government environment. The customer-hosted enclave is distinct from the compliance platform. The customer still needs the documented infrastructure, license and operating skills.

AIC references: air gapped · security · shared responsibility

CQ21 · Deployment and customer control

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Vanta: The published material reviewed for Vanta does not specify fully disconnected operation, including license validation, authentication and updates. Require an offline test rather than infer air-gap support from self-hosting or a local agent. Document which functions stop when external connectivity is removed.

Drata: The published material reviewed for Drata does not specify fully disconnected operation, including license validation, authentication and updates. Require an offline test rather than infer air-gap support from self-hosting or a local agent. Document which functions stop when external connectivity is removed.

Secureframe: The published material reviewed for Secureframe does not specify fully disconnected operation, including license validation, authentication and updates. Require an offline test rather than infer air-gap support from self-hosting or a local agent. Document which functions stop when external connectivity is removed.

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.

Vanta: The offering reviewed is a cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places. The reviewed architecture does not fully resolve storage/replication locations for credentials, evidence, logs and backups. Obtain the data-flow and hosting schedule for the exact edition, including subprocessors and optional integrations.

Drata: The offering reviewed is a cloud compliance platform. Select the specific product and edition before assigning hosting responsibilities; managed assets and the management platform can be in different places. The reviewed architecture does not fully resolve storage/replication locations for credentials, evidence, logs and backups. Obtain the data-flow and hosting schedule for the exact edition, including subprocessors and optional integrations.

Secureframe: Secureframe provides cloud compliance workflows and Defense Navigator provisioning in the customer’s Azure Government environment. The customer-hosted enclave is distinct from the compliance platform. The reviewed architecture does not fully resolve storage/replication locations for credentials, evidence, logs and backups. Obtain the data-flow and hosting schedule for the exact edition, including subprocessors and optional integrations.

AIC references: air gapped · security · shared responsibility

CQ23 · Deployment and customer control

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Vanta: The published material reviewed for Vanta does not specify the exact supplier-support access, key custody and privileged access approval controls for the proposed tenant. Request the access model and contractual commitments, including support elevation, audit records and subprocessors. SaaS does not by itself mean the customer has no data control.

Drata: The published material reviewed for Drata does not specify the exact supplier-support access, key custody and privileged access approval controls for the proposed tenant. Request the access model and contractual commitments, including support elevation, audit records and subprocessors. SaaS does not by itself mean the customer has no data control.

Secureframe: The published material reviewed for Secureframe does not specify the exact supplier-support access, key custody and privileged access approval controls for the proposed tenant. Request the access model and contractual commitments, including support elevation, audit records and subprocessors. SaaS does not by itself mean the customer has no data control.

AIC references: air gapped · security · shared responsibility

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.

Vanta: Vanta documents exports from most platform areas. Its People export excludes training records held in third-party integrations. Preserve those records separately and test the exported control/history relationships before terminating the service.

Drata: The published material reviewed for Drata does not specify complete export coverage, formats, retained history and post-termination access for this package. Request a sample export of attachments, approvals, timestamps and control relationships; compare it with the exit clause before cancelling.

Secureframe: The published material reviewed for Secureframe does not specify complete export coverage, formats, retained history and post-termination access for this package. Request a sample export of attachments, approvals, timestamps and control relationships; compare it with the exit clause before cancelling.

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Vanta: The published material reviewed for Vanta does not specify the intended MSP's administrative rights, customer tenancy rights and exit access under this contract. Assign roles in writing and test customer access to evidence without depending on one MSP employee. Managed/co-managed programs may have different boundaries.

Drata: The published material reviewed for Drata does not specify the intended MSP's administrative rights, customer tenancy rights and exit access under this contract. Assign roles in writing and test customer access to evidence without depending on one MSP employee. Managed/co-managed programs may have different boundaries.

Secureframe: The published material reviewed for Secureframe does not specify the intended MSP's administrative rights, customer tenancy rights and exit access under this contract. Assign roles in writing and test customer access to evidence without depending on one MSP employee. Managed/co-managed programs may have different boundaries.

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.

Vanta: The published material reviewed for Vanta does not specify the exact behavior of every component during a service or connectivity outage. Obtain availability/recovery commitments and test authentication, existing sessions, evidence access and emergency administration. An uptime percentage alone does not describe operational continuity.

Drata: The published material reviewed for Drata does not specify the exact behavior of every component during a service or connectivity outage. Obtain availability/recovery commitments and test authentication, existing sessions, evidence access and emergency administration. An uptime percentage alone does not describe operational continuity.

Secureframe: The published material reviewed for Secureframe does not specify the exact behavior of every component during a service or connectivity outage. Obtain availability/recovery commitments and test authentication, existing sessions, evidence access and emergency administration. An uptime percentage alone does not describe operational continuity.

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Vanta: Select the environment around actual FCI/CUI workflows. Neither a cloud subscription nor a governance tool defines all assets in scope. The comparison must include systems that process the data and systems providing their protection; the final boundary follows the applicable scoping guidance.

Drata: Select the environment around actual FCI/CUI workflows. Neither a cloud subscription nor a governance tool defines all assets in scope. The comparison must include systems that process the data and systems providing their protection; the final boundary follows the applicable scoping guidance.

Secureframe: Select the environment around actual FCI/CUI workflows. Neither a cloud subscription nor a governance tool defines all assets in scope. The comparison must include systems that process the data and systems providing their protection; the final boundary follows the applicable scoping guidance.

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.

Vanta: The published material reviewed for Vanta does not specify a current requirement-by-requirement allocation for the selected complete customer configuration. Obtain the shared-responsibility/control matrix with performed, assisted and customer-owned activities. Do not rank suppliers by percentages that use different denominators.

Drata: Drata's CMMC description includes shared controls, evidence, owners and POA&M oversight. That is compliance-program support; obtain the customer's actual control/responsibility matrix to distinguish documentation from operating controls.

Secureframe: The published material reviewed for Secureframe does not specify a current requirement-by-requirement allocation for the selected complete customer configuration. Obtain the shared-responsibility/control matrix with performed, assisted and customer-owned activities. Do not rank suppliers by percentages that use different denominators.

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.

Vanta: The customer retains responsibility for scope, authorized users, organizational procedures and the systems outside the purchased service. Assign integration, remediation and evidence-review duties explicitly to the customer, MSP and supplier.

Drata: The customer retains responsibility for scope, authorized users, organizational procedures and the systems outside the purchased service. Assign integration, remediation and evidence-review duties explicitly to the customer, MSP and supplier.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Secureframe: The customer retains responsibility for scope, authorized users, organizational procedures and the systems outside the purchased service. Assign integration, remediation and evidence-review duties explicitly to the customer, MSP and supplier.

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.

Vanta: Vanta collects evidence through integrations and runs automated tests. Coverage depends on connected systems and the required artifact; retain separately collected organizational records and inspect failed/stale checks.

Drata: Drata describes continuous evidence and control monitoring. Connector coverage and control ownership determine what is collected automatically; organizational procedures and unconnected systems still need evidence owners.

Secureframe: Configuration evidence feeds automated tests; personnel and configuration data remain synchronized. Policies and other organizational evidence still have separate owners.

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.

Vanta: The published material reviewed for Vanta does not specify which corrective actions execute directly on the customer’s target systems. Demonstrate one failed check through authorization, actual correction, verification and evidence; distinguish an assigned ticket from an executed repair. Establish the check cadence and the owner of exceptions between assessments.

Drata: Drata describes control testing, linked evidence, ownership and POA&M oversight. Those workflows do not establish which changes it executes on your specific hosts; require an actual failing-control repair demonstration. Establish the check cadence and the owner of exceptions between assessments.

Secureframe: Navigator continuously tests configuration and flags drift. The setup guide does not establish automatic repair of every subsequent deviation; test the required correction path.

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.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Vanta: The published material reviewed for Vanta does not specify all four workflows-training, attestations, access approvals and corrective actions-in the selected package. Request each workflow and its retained records separately. Policy acknowledgement does not establish a full training program, and a task list does not establish access enforcement.

Drata: The published material reviewed for Drata does not specify all four workflows-training, attestations, access approvals and corrective actions-in the selected package. Request each workflow and its retained records separately. Policy acknowledgement does not establish a full training program, and a task list does not establish access enforcement.

Secureframe: The published material reviewed for Secureframe does not specify all four workflows-training, attestations, access approvals and corrective actions-in the selected package. Request each workflow and its retained records separately. Policy acknowledgement does not establish a full training program, and a task list does not establish access enforcement.

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.

Vanta: The GRC/audit role supports organizing review material, but exact auditor permissions and disclosure controls must be demonstrated. Test limited reviewer access, export and evidence freshness without granting operational administrator rights.

Drata: The GRC/audit role supports organizing review material, but exact auditor permissions and disclosure controls must be demonstrated. Test limited reviewer access, export and evidence freshness without granting operational administrator rights.

Secureframe: The GRC/audit role supports organizing review material, but exact auditor permissions and disclosure controls must be demonstrated. Test limited reviewer access, export and evidence freshness without granting operational administrator rights.

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.

Vanta: Vanta’s framework mappings support reusing control evidence across compliance programs. Check which frameworks and modules are included in the quote and whether the same artifact supports each applicable scope.

Drata: The offering’s framework/control workflows may support reuse. Verify the actual frameworks, editions and crosswalks you need; reusing one control record is not the same as treating different standards as identical.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Secureframe: The offering's framework/control workflows may support reuse. Verify the actual frameworks, editions and crosswalks you need; reusing one control record is not the same as treating different standards as identical.

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.

Vanta: Retain useful SaaS integrations and trust workflows; compare overlapping audit and evidence functions before retiring them. An integration needs an identified API/export, matching control identifiers and an owner; a generic partnership claim is not a working data connection.

Drata: Keep enterprise-wide compliance programs in Drata where they serve broader obligations; supply operational evidence through an agreed interface. An integration needs an identified API/export, matching control identifiers and an owner; a generic partnership claim is not a working data connection.

Secureframe: Evaluate Defense enclave provisioning separately from compliance workflows. Secureframe is not merely a document checklist. An integration needs an identified API/export, matching control identifiers and an owner; a generic partnership claim is not a working data connection.

AIC references: supported platforms · requirements mapping

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.

Vanta: Vanta publishes plan/package information and directs buyers to a scoped quote. Obtain framework, integration, trust and risk module entitlements rather than assume one flat license covers the program. Add infrastructure, operating staff, migration, retention and assessment costs that are outside that quote. Compare the same workloads and service hours.

Drata: The published material reviewed for Drata does not specify a complete current price and license-meter schedule for this customer configuration. Obtain the edition, quantities, add-ons, implementation, recurring support and renewal terms in one itemized quote. Add infrastructure, operating staff, migration, retention and assessment costs that are outside that quote. Compare the same workloads and service hours.

Secureframe: Defense is a separate package above the other published tiers; its scope includes enclave and CMMC documentation functions. Obtain separate Azure consumption, desktops, support and implementation costs. Add infrastructure, operating staff, migration, retention and assessment costs that are outside that quote. Compare the same workloads and service hours.

AIC references: pricing · pricing

CQ37 · Cost and value

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Vanta: Vanta publishes plan/package information and directs buyers to a scoped quote. Obtain framework, integration, trust and risk module entitlements rather than assume one flat license covers the program.

Drata: The published material reviewed for Drata does not specify a complete current price and license-meter schedule for this customer configuration. Obtain the edition, quantities, add-ons, implementation, recurring support and renewal terms in one itemized quote.

Secureframe: Defense is a separate package above the other published tiers; its scope includes enclave and CMMC documentation functions. Obtain separate Azure consumption, desktops, support and implementation costs.

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.

Vanta: The published material reviewed for Vanta does not specify a separate non-human-identity charge or an explicit exemption in the selected license. Ask how service identities, application accounts, secrets, managed targets and API usage are counted. Do not assume a people-seat price includes every machine identity.

Drata: The published material reviewed for Drata does not specify a separate non-human-identity charge or an explicit exemption in the selected license. Ask how service identities, application accounts, secrets, managed targets and API usage are counted. Do not assume a people-seat price includes every machine identity.

Secureframe: The published material reviewed for Secureframe does not specify a separate non-human-identity charge or an explicit exemption in the selected license. Ask how service identities, application accounts, secrets, managed targets and API usage are counted. Do not assume a people-seat price includes every machine identity.

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.

Vanta: Vanta publishes plan/package information and directs buyers to a scoped quote. Obtain framework, integration, trust and risk module entitlements rather than assume one flat license covers the program. Have the supplier identify optional connectors, reporting, storage, reviewer seats and support explicitly as included or separately charged.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: The published material reviewed for Drata does not specify a complete current price and license-meter schedule for this customer configuration. Obtain the edition, quantities, add-ons, implementation, recurring support and renewal terms in one itemized quote. Have the supplier identify optional connectors, reporting, storage, reviewer seats and support explicitly as included or separately charged.

Secureframe: Defense is a separate package above the other published tiers; its scope includes enclave and CMMC documentation functions. Obtain separate Azure consumption, desktops, support and implementation costs. Have the supplier identify optional connectors, reporting, storage, reviewer seats and support explicitly as included or separately charged.

AIC references: pricing · pricing

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.

Vanta: List the server/service prerequisites, identity integration, storage, backup and third-party applications for the selected architecture. A documented product capability does not prove the customer already owns its dependencies.

Drata: List the server/service prerequisites, identity integration, storage, backup and third-party applications for the selected architecture. A documented product capability does not prove the customer already owns its dependencies.

Secureframe: List the server/service prerequisites, identity integration, storage, backup and third-party applications for the selected architecture. A documented product capability does not prove the customer already owns its dependencies.

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.

Vanta: No independently verified staffing estimate for your Vanta deployment is established here. Measure setup, connector maintenance, exception handling, evidence review and update work during the pilot. Managed-service labor belongs in the contract, not an assumed zero-hour estimate.

Drata: No independently verified staffing estimate for your Drata deployment is established here. Measure setup, connector maintenance, exception handling, evidence review and update work during the pilot. Managed-service labor belongs in the contract, not an assumed zero-hour estimate.

Secureframe: No independently verified staffing estimate for your Secureframe deployment is established here. Measure setup, connector maintenance, exception handling, evidence review and update work during the pilot. Managed-service labor belongs in the contract, not an assumed zero-hour estimate.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Vanta: Potential consolidation follows the documented scope: CMMC workflows, evidence automation, control monitoring and framework mapping. Identify the exact existing task or subscription replaced and the records it preserves. Avoid double-counting savings while keeping the same staff work or another required module.

Drata: Potential consolidation follows the documented scope: CMMC controls, continuous evidence and defined ownership across compliance programs. Identify the exact existing task or subscription replaced and the records it preserves. Avoid double-counting savings while keeping the same staff work or another required module.

Secureframe: Potential consolidation follows the documented scope: Defense Navigator, SSP workflows and automated CUI enclave configuration in customer-owned cloud environments. Identify the exact existing task or subscription replaced and the records it preserves. Avoid double-counting savings while keeping the same staff work or another required module.

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.

Vanta: Vanta publishes plan/package information and directs buyers to a scoped quote. Obtain framework, integration, trust and risk module entitlements rather than assume one flat license covers the program. Model growth using additional users/tenants/assets, workload capacity, retained evidence and support scope. Verify renewal and overage terms instead of assuming the initial unit rate remains constant.

Drata: The published material reviewed for Drata does not specify a complete current price and license-meter schedule for this customer configuration. Obtain the edition, quantities, add-ons, implementation, recurring support and renewal terms in one itemized quote. Model growth using additional users/tenants/assets, workload capacity, retained evidence and support scope. Verify renewal and overage terms instead of assuming the initial unit rate remains constant.

Secureframe: Defense is a separate package above the other published tiers; its scope includes enclave and CMMC documentation functions. Obtain separate Azure consumption, desktops, support and implementation costs. Model growth using additional users/tenants/assets, workload capacity, retained evidence and support scope. Verify renewal and overage terms instead of assuming the initial unit rate remains constant.

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.

Vanta: A hosted VDI capacity allowance is not established as part of the offering reviewed. If VDI is added through another product or provider, its compute, storage, concurrency and usage terms belong in a separate line of the comparison.

Drata: A hosted VDI capacity allowance is not established as part of the offering reviewed. If VDI is added through another product or provider, its compute, storage, concurrency and usage terms belong in a separate line of the comparison.

Secureframe: Secureframe’s desktop provisioning documentation includes enclave sizing and a shared data drive. Obtain the actual VM sizes, concurrency, application licensing and Azure charges for the proposed configuration; those are not implied by the compliance subscription.

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.

Vanta: Export control mappings, evidence history and owner assignments; prove that the replacement preserves required audit workflows. Distinguish integrating existing systems from moving the workload into a new boundary; they involve different change and migration effort.

Drata: Map shared controls and evidence retention first, then pilot one scope before changing the compliance system of record. Distinguish integrating existing systems from moving the workload into a new boundary; they involve different change and migration effort.

Secureframe: Preserve the cloud boundary and SSP, then test supported operating systems, administrative paths and evidence exports before changing platforms. Distinguish integrating existing systems from moving the workload into a new boundary; they involve different change and migration effort.

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.

Vanta: The published material reviewed for Vanta does not specify a reproducible end-to-end enclave deployment time for your architecture. Ask for measured provisioning prerequisites and distinguish instance creation from configuration, data transfer, training and operational handover. For a GRC or assessment-only purchase, enclave provisioning is a separate project.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: The published material reviewed for Drata does not specify a reproducible end-to-end enclave deployment time for your architecture. Ask for measured provisioning prerequisites and distinguish instance creation from configuration, data transfer, training and operational handover. For a GRC or assessment-only purchase, enclave provisioning is a separate project.

Secureframe: Secureframe documents connecting an Azure Government environment and provisioning virtual desktops through Defense Navigator. The reviewed instructions do not establish a universal customer deployment duration; measure prerequisites, sizing and provisioning separately from onboarding.

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.

Vanta: No validated deployment-wide discovery/remediation duration for Vanta is available here. Reachability, privileges, integrations and change approval determine elapsed time. Require a representative discovery sample and a plan for exceptions rather than adopt a marketing launch-time claim.

Drata: No validated deployment-wide discovery/remediation duration for Drata is available here. Reachability, privileges, integrations and change approval determine elapsed time. Require a representative discovery sample and a plan for exceptions rather than adopt a marketing launch-time claim.

Secureframe: No validated deployment-wide discovery/remediation duration for Secureframe is available here. Reachability, privileges, integrations and change approval determine elapsed time. Require a representative discovery sample and a plan for exceptions rather than adopt a marketing launch-time claim.

AIC references: supported platforms · requirements mapping

CQ48 · Implementation and migration

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.

Vanta: Export control mappings, evidence history and owner assignments; prove that the replacement preserves required audit workflows. Stage the change with acceptance tests, retained records and rollback. If the offering requires a new service boundary, include the interim data path and access dependencies in the pilot.

Drata: Map shared controls and evidence retention first, then pilot one scope before changing the compliance system of record. Stage the change with acceptance tests, retained records and rollback. If the offering requires a new service boundary, include the interim data path and access dependencies in the pilot.

Secureframe: Preserve the cloud boundary and SSP, then test supported operating systems, administrative paths and evidence exports before changing platforms. Stage the change with acceptance tests, retained records and rollback. If the offering requires a new service boundary, include the interim data path and access dependencies in the pilot.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Vanta: Export control mappings, evidence history and owner assignments; prove that the replacement preserves required audit workflows. Preserve source evidence and timestamp/owner relationships. Validate the import and credential-change behavior before deleting or terminating any original service.

Drata: Map shared controls and evidence retention first, then pilot one scope before changing the compliance system of record. Preserve source evidence and timestamp/owner relationships. Validate the import and credential-change behavior before deleting or terminating any original service.

Secureframe: Preserve the cloud boundary and SSP, then test supported operating systems, administrative paths and evidence exports before changing platforms. Preserve source evidence and timestamp/owner relationships. Validate the import and credential-change behavior before deleting or terminating any original 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.

Vanta: The customer retains responsibility for scope, authorized users, organizational procedures and the systems outside the purchased service. Assign integration, remediation and evidence-review duties explicitly to the customer, MSP and supplier. The purchase must identify who executes the migration and who accepts the resulting environment.

Drata: The customer retains responsibility for scope, authorized users, organizational procedures and the systems outside the purchased service. Assign integration, remediation and evidence-review duties explicitly to the customer, MSP and supplier. The purchase must identify who executes the migration and who accepts the resulting environment.

Secureframe: The customer retains responsibility for scope, authorized users, organizational procedures and the systems outside the purchased service. Assign integration, remediation and evidence-review duties explicitly to the customer, MSP and supplier. The purchase must identify who executes the migration and who accepts the resulting environment.

AIC references: supported platforms · requirements mapping

CQ51 · Implementation and migration

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Vanta: The published material reviewed for Vanta does not specify the complete included training, deployment assistance, support hours and response commitments for this package. Obtain the named support schedule and training deliverables. Distinguish a response target from a resolution commitment and product support from managed operations.

Drata: The published material reviewed for Drata does not specify the complete included training, deployment assistance, support hours and response commitments for this package. Obtain the named support schedule and training deliverables. Distinguish a response target from a resolution commitment and product support from managed operations.

Secureframe: The published material reviewed for Secureframe does not specify the complete included training, deployment assistance, support hours and response commitments for this package. Obtain the named support schedule and training deliverables. Distinguish a response target from a resolution commitment and product support from managed operations.

AIC references: supported platforms · requirements mapping

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.

Vanta: The published material reviewed for Vanta does not specify a trial entitlement on your own systems with the required modules and duration. Request a scoped evaluation with agreed targets, license terms, success criteria and cleanup. A sales demo is not automatically permission to run a production pilot.

Drata: The published material reviewed for Drata does not specify a trial entitlement on your own systems with the required modules and duration. Request a scoped evaluation with agreed targets, license terms, success criteria and cleanup. A sales demo is not automatically permission to run a production pilot.

Secureframe: The published material reviewed for Secureframe does not specify a trial entitlement on your own systems with the required modules and duration. Request a scoped evaluation with agreed targets, license terms, success criteria and cleanup. A sales demo is not automatically permission to run a production pilot.

AIC references: supported platforms · requirements mapping

CQ53 · Vendor credibility and fit

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Who is this company, and how long has it supported this kind 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.

Vanta: Vanta is represented here by its published Cloud compliance platform offering. The reviewed evidence does not establish an independently checked duration of support for your exact environment; ask for relevant delivery history rather than infer it from brand age.

Drata: Drata is represented here by its published Cloud compliance platform offering. The reviewed evidence does not establish an independently checked duration of support for your exact environment; ask for relevant delivery history rather than infer it from brand age.

Secureframe: Secureframe is represented here by its published Compliance platform with customer-cloud enclave provisioning offering. The reviewed evidence does not establish an independently checked duration of support for your exact environment; ask for relevant delivery history rather than infer it from brand age.

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.

Vanta: The relevant fit question is: Your evidence is collected, but privileged changes still happen outside the compliance workflow. Ask the supplier for a reference architecture and customer reference matching your system mix, operating team and regulatory scope.

Drata: The relevant fit question is: Teams answer the same control question in several systems while administrators work in another. Ask the supplier for a reference architecture and customer reference matching your system mix, operating team and regulatory scope.

Secureframe: The relevant fit question is: A cloud enclave may cover the office workflow while factory systems and privileged accounts still need controls. Ask the supplier for a reference architecture and customer reference matching your system mix, operating team and regulatory scope.

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.

Vanta: Show a failed configuration check, its authorized repair and the evidence attached to the same control. Require the supplier to perform the comparable workflow on its proposed edition and retain the observed result.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Drata: Trace an access approval through session activity, revocation and the resulting evidence. Require the supplier to perform the comparable workflow on its proposed edition and retain the observed result.

Secureframe: Use an on-premises administrative session to show the difference between cloud provisioning and control of the customer's wider environment. Require the supplier to perform the comparable workflow on its proposed edition and retain the observed result.

AIC references: supported platforms · requirements mapping

CQ56 · Vendor credibility and fit

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.

Vanta: This review does not contain independently verified Vanta customer interviews or support-performance measurements. Supplier case studies can identify references, but are not a substitute for speaking with a comparable customer and reviewing the contracted service terms.

Drata: This review does not contain independently verified Drata customer interviews or support-performance measurements. Supplier case studies can identify references, but are not a substitute for speaking with a comparable customer and reviewing the contracted service terms.

Secureframe: This review does not contain independently verified Secureframe customer interviews or support-performance measurements. Supplier case studies can identify references, but are not a substitute for speaking with a comparable customer and reviewing the contracted service terms.

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.

Vanta: The documented scope is a cloud compliance platform, with edition-specific limits. Unverified target support, export completeness, outage behavior and contractual entitlements remain explicit procurement checks; resolve them in the technical evaluation and contract.

Drata: The documented scope is a cloud compliance platform, with edition-specific limits. Unverified target support, export completeness, outage behavior and contractual entitlements remain explicit procurement checks; resolve them in the technical evaluation and contract.

Secureframe: The documented scope is Compliance platform with customer-cloud enclave provisioning, with edition-specific limits. Unverified target support, export completeness, outage behavior and contractual entitlements remain explicit procurement checks; resolve them in the technical evaluation and contract.

AIC references: supported platforms · requirements mapping

CQ58 · Vendor credibility and fit

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Vanta: The published offering currently describes CMMC workflows, evidence automation, control monitoring and framework mapping. Any feature discussed only as roadmap or without an orderable edition should stay outside the scored current comparison until release documentation and a demonstration establish delivery.

Drata: The published offering currently describes CMMC controls, continuous evidence and defined ownership across compliance programs. Any feature discussed only as roadmap or without an orderable edition should stay outside the scored current comparison until release documentation and a demonstration establish delivery.

Secureframe: The published offering currently describes Defense Navigator, SSP workflows and automated CUI enclave configuration in customer-owned cloud environments. Any feature discussed only as roadmap or without an orderable edition should stay outside the scored current comparison until release documentation and a demonstration establish delivery.

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.

Vanta: The published material reviewed for Vanta does not specify the exact vulnerability notification, update timing and emergency patch process applicable to this deployment. Obtain the security advisory channel, support policy and maintenance responsibilities. For self-hosted components, test the customer update process; for managed services, specify supplier notification and evidence duties.

Drata: The published material reviewed for Drata does not specify the exact vulnerability notification, update timing and emergency patch process applicable to this deployment. Obtain the security advisory channel, support policy and maintenance responsibilities. For self-hosted components, test the customer update process; for managed services, specify supplier notification and evidence duties.

Secureframe: The published material reviewed for Secureframe does not specify the exact vulnerability notification, update timing and emergency patch process applicable to this deployment. Obtain the security advisory channel, support policy and maintenance responsibilities. For self-hosted components, test the customer update process; for managed services, specify supplier notification and evidence duties.

AIC references: security

CQ60 · Vendor credibility and fit

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

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.

Vanta: Retain useful SaaS integrations and trust workflows; compare overlapping audit and evidence functions before retiring them. Validate the specific connector, export format or service relationship and its permissions before presenting coexistence as turnkey.

Drata: Keep enterprise-wide compliance programs in Drata where they serve broader obligations; supply operational evidence through an agreed interface. Validate the specific connector, export format or service relationship and its permissions before presenting coexistence as turnkey.

Secureframe: Evaluate Defense enclave provisioning separately from compliance workflows. Secureframe is not merely a document checklist. Validate the specific connector, export format or service relationship and its permissions before presenting coexistence as turnkey.

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.

Vanta: An acquisition or strategy change does not by itself determine your rights. The reviewed Vanta material does not establish a perpetual right to use all components or a complete exit guarantee. Retain the current agreement, renewal/termination provisions, exports and a tested continuity plan.

Drata: An acquisition or strategy change does not by itself determine your rights. The reviewed Drata material does not establish a perpetual right to use all components or a complete exit guarantee. Retain the current agreement, renewal/termination provisions, exports and a tested continuity plan.

Secureframe: An acquisition or strategy change does not by itself determine your rights. The reviewed Secureframe material does not establish a perpetual right to use all components or a complete exit guarantee. Retain the current agreement, renewal/termination provisions, exports and a tested continuity plan.

AIC references: supported platforms · requirements mapping

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Sources and scope

Deployment and customer-control statements reflect the product owner’s November 20, 2026 instructions and AIC’s documented deployment model. Supplier answers retain the separate published October 17, 2026 analyses; they are not a newly performed independent benchmark.

- 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://www.vanta.com/products/cmmc
- https://help.vanta.com/en/articles/14998654-exporting-your-data-from-vanta
- https://www.vanta.com/pricing
- https://analoginfo.com/pricing
- https://analoginfo.com/downloads
- https://dodcio.defense.gov/Portals/0/Documents/CMMC/ScopingGuideL2v2.pdf
- https://analoginfo.com/aic-enterprise-privilege-suite
- https://analoginfo.com/aic-cmmc-complete
- https://analoginfo.com/contact-sales
- https://drata.com/product/cmmc
- https://drata.com/continuous-compliance-data-sheet
- https://support.secureframe.com/en/articles/16597330-cui-enclave-setup
- https://support.secureframe.com/en/articles/16632215-provisioning-virtual-desktops
- https://secureframe.com/pricing

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.