Analog Informatics™ Corporation

AIC Hosting Models and Shared Responsibilities for CMMC Assessments

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

analoginfo.com

Revised 29 October 2026

View this resource online

AIC hosting responsibilities depend on the deployment model. The Customer Responsibility Matrix (CRM) below identifies the duties of the cloud provider, Analog Informatics Corporation (AIC), the customer, and any Managed Service Provider (MSP).

Shared responsibilities apply across Governance, Risk, and Compliance (GRC) programs. Cybersecurity Maturity Model Certification (CMMC) names them External Service Provider (ESP) and Cloud Service Provider (CSP) in 32 CFR Part 170 Table 4. Federal Risk and Authorization Management Program (FedRAMP) and Government Community Cloud (GCC) use a CRM on an authorization boundary. Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), System and Organization Controls 2 (SOC 2), ISO/IEC 27001, and operational technology programs use the same split under different names.

AIC is not the CSP. AIC is not a Managed Service Provider (MSP). There are three ways to host AIC. In the first two, you run pre-installed AIC software. In the third, AIC runs as an authorized application under a third-party cloud provider's FedRAMP or GCC authorization. A control-level CRM is provided with the kit or hosted-application engagement. The three hosting models apply to CMMC and the other frameworks on Frameworks.

AIC offers two products: AIC Enterprise Privilege Suite™ and AIC CMMC Complete™.

Direct Answers

Question	Answer
Are you a Cloud Service Provider (CSP)?	No. When a cloud is in use, that cloud provider is the CSP. AIC is software, or an authorized application on that provider's authorization.
Are you an External Service Provider (ESP), processor, or service organization?	No in on-premises hosting and in commercial Infrastructure as a Service (IaaS) hosting. You run AIC. Regulated data stays in the environment you control. In FedRAMP or GCC hosting, AIC is an authorized application under the cloud provider's authority. If an MSP operates the environment, that MSP may be the ESP, processor, or service organization under the framework you use.
Are you a Managed Service Provider (MSP)?	No. AIC supports MSPs and cloud providers. AIC does not replace your MSP.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Question	Answer
Do you hold a FedRAMP authorization?	No. In FedRAMP or GCC hosting, AIC operates under the cloud provider's authorization as an authorized application.
Is a Customer Responsibility Matrix (CRM) available?	Yes. This page is the public summary for every framework the suite maps. A control-level CRM is provided with the kit or hosted-application engagement.
Is CMMC the only framework?	No. CMMC is one of many. The same tools cover FedRAMP, GCC, National Institute of Standards and Technology (NIST) catalogs, PCI DSS, GDPR, HIPAA, SOC 2, ISO/IEC 27001, HITRUST, IEC 62443, North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP), and most other GRC frameworks.

Security and Continuous Compliance

Continuous compliance is always the best operating strategy. A FedRAMP or GCC authorization covers the cloud. It does not configure privileged accounts, rotate credentials, broker sessions, train the workforce, or keep the evidence an assessor reads. AIC adds the application, identity, privilege, evidence, and workforce layer that sits on top of the environment you choose.

Feeds, alerts, repair paths, and rescans run between assessments.

AIC Security Capabilities

- Software: AIC Enterprise Privilege Suite™ and AIC CMMC Complete™
- Processes and procedures you run in the product
- Privileged Identity Management (PIM) and Privileged Access Management (PAM)
- Credential rotation, just-in-time elevation, and recorded sessions
- Incident Response playbooks, detectors, and records
- Workforce training and signed attestation
- Evidence collection and the Assessment Binder
- Auditor tools: Current State Compliance, living binder sections, and export

Supported framework mappings include CMMC, NIST Special Publication (SP) 800-171, NIST SP 800-172, NIST SP 800-53, PCI DSS, GDPR, ISO/IEC 27001, SOC 2,

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

HITRUST, HIPAA, California privacy, IEC 62443, NERC CIP, Australian Essential Eight, and NIS2.

See Capabilities and Frameworks.

Three Ways to Host AIC

1. On premises

You use your own internal hardware, software, and networking. AIC software provides the controls, the records, and the auditor tools.

- You own the site, the network, and the hosts.
- You run AIC.
- You exclusively control the environment, the cryptography, and access.
- AIC licenses software. AIC does not host your data and has no standing access.
- AIC is not the ESP and not the CSP.

2. Commercial cloud as Infrastructure as a Service

You use a commercial cloud that is not FedRAMP or GCC. The cloud supplies infrastructure only: compute, storage, and network. You do not use that provider's managed services.

You stand up a secure enclave on Security Technical Implementation Guide (STIG) hardened virtual machines, with a public and private network that you define. The environment, the cryptography, and access are exclusively yours.

- AIC software is pre-installed in that enclave.
- You run AIC. AIC does not operate the enclave.
- The commercial cloud supplies infrastructure only.
- AIC is not the ESP and not the CSP.

3. FedRAMP or GCC authorized cloud

You use a third-party cloud provider that holds FedRAMP or GCC authorization. AIC provides software in that environment for cybersecurity and GRC.

- The cloud provider remains the CSP.
- AIC operates under that provider's authority as an authorized application.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

- AIC does not replace the provider's authorization and does not hold its own FedRAMP authorization.
- AIC is not the CSP.
- AIC is not an MSP.
- Shared duties are written in a CRM that sits next to the cloud provider's CRM.

If an MSP operates the environment for a customer, that MSP may be the ESP. AIC still is not the MSP.

AIC supports existing cloud providers on GCC and FedRAMP offerings, and supports MSPs that serve those customers. The authorization stays with the provider. AIC supplies the cybersecurity and GRC application on that authorized cloud.

Who This Is For

- Cloud providers, large and small, that already offer FedRAMP or GCC and want the application, identity, privilege, evidence, and workforce layer as an authorized application on that authorization
- Enterprises and agencies that need privileged access, identity, evidence, and continuous compliance on premises, on commercial IaaS, or on an authorized cloud
- Payment, healthcare, privacy, and operational technology programs that use the same stack under PCI DSS, HIPAA, GDPR, IEC 62443, or NERC CIP
- Small and medium-sized businesses (SMBs) working toward FedRAMP, GCC, CMMC, ISO/IEC 27001, SOC 2, and most other GRC frameworks
- MSPs that AIC supports. AIC licenses software and, in FedRAMP or GCC hosting, can run as an authorized application. AIC does not take the customer relationship or the managed-service role. See Managed Service Providers.

Customer Responsibility Matrix

We provide a Customer Responsibility Matrix that assigns Cloud provider, Analog Informatics, Customer, and MSP duties. The table below is the public summary. A detailed control-level CRM is provided with the kit or hosted-application engagement.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Duty	Cloud provider	Analog Informatics	You (customer)	Your MSP (if you use one)
Data center and hypervisor	On premises: none. Commercial IaaS: facility and hypervisor only. FedRAMP or GCC: owns and authorizes the facility, hardware, and hypervisor	Does not operate the data center	On premises: owns the site. Cloud models: chooses the cloud	Not the data center
Identity of the cloud tenant	On premises: none. Cloud models: issues the tenant	Does not own the tenant	Owns the tenant, billing, and tenant administrators, or owns the on-premises directory	May administer the tenant if you delegate
Application hosting	On premises: none. Commercial IaaS: compute, storage, and network only. No managed services. FedRAMP or GCC: authorized compute, storage, and network	On premises and commercial IaaS: licenses pre-installed software you run. FedRAMP or GCC: authorized application under the provider's authority	Chooses the hosting model. In models 1 and 2, you run AIC	May install or operate the application if you hire them
Privileged identity and session control	Cloud control-plane identity when a cloud is used	PIM and PAM for the accounts and sessions the suite manages	Sets who may be privileged and approves access	May operate privileged access if you delegate
Credential rotation and elevation	Platform credentials the provider manages, if any	Discovers, vaults, rotates, and elevates credentials the suite manages	Owns the accounts and the rotation policy	May run rotation jobs if you delegate

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Duty	Cloud provider	Analog Informatics	You (customer)	Your MSP (if you use one)
Workforce training and attestation	Provider workforce for the cloud, if any	Assigns training, collects signed attestation, and keeps the record	Names the people in scope and the due dates	May assign training for your people if you hire them
Incident Response playbooks and records	Provider incident process for the cloud, if any	Incident Response playbooks, detectors, and records in the product	Owns your incident process and your reporting	May operate Incident Response if you hire them
Evidence collection and auditor binder	Provider evidence for the cloud, if any	Assessment Binder, Current State Compliance, and live evidence	Owns the evidence package you present	Shares the binder when you grant access
System Security Plan, policies, and assessment	Provider authorization package for a FedRAMP or GCC cloud	Product documentation, Assessment Binder, and the Customer Responsibility Matrix	Owns your plan, your policies, and the assessment you present	May help prepare the package if you hire them
Regulated data handling	Provider handling rules when that data is in a FedRAMP or GCC cloud	Marking, vault, governed mail, access, and records for data the suite holds: Controlled Unclassified Information (CUI), Federal Contract Information (FCI), cardholder data, protected health information, personal data, and operational technology access records	Owns the policy: who may handle which data, and where	Follows your policy

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Duty	Cloud provider	Analog Informatics	You (customer)	Your MSP (if you use one)
Who holds encryption keys	May offer a hardware security module (HSM) or key management service. In commercial IaaS you do not use those managed services	Encrypts with the keys you designate. Does not take ownership of your keys	You exclusively control cryptography. Keys live in software, an HSM, or a key service you own	Only if you delegate key custody

Shared Responsibility by Framework

AIC supplies privileged identity, privileged access, configuration compliance, Incident Response records, workforce training, evidence, and auditor tools. You own policy, people, facilities, and the assessment outcome. The cloud provider, when you use one, owns the facility and hypervisor. In model 3, that provider also holds the cloud authorization.

An assessment organization, certification body, or regulator decides whether a requirement is satisfied. These rows describe product availability and ownership. They are not an assessment result.

Framework	What they call the split	What AIC supplies	What stays with you	Page
FedRAMP and GCC	Customer Responsibility Matrix on the cloud authorization boundary	Authorized application layer: identity, privilege, sessions, evidence, training, Incident Response records	Tenant, keys, who is in scope, and the package you present. The cloud provider holds the authorization	Public sector, Government deployment
CMMC, NIST SP 800-171, NIST SP 800-172	ESP and CSP under 32 CFR Part 170 Table 4 to section 170.19(c)(2)(i)	Controls, training, and Assessment Binder records for CUI and FCI the suite holds	System Security Plan, physical and personnel duties, and the assessment	CMMC, NIST SP 800-171, NIST SP 800-172

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Framework	What they call the split	What AIC supplies	What stays with you	Page
NIST SP 800-53	Shared control inheritance: common, inherited, and organization-defined	Access, audit, identity, configuration, Incident Response, and monitoring on systems the suite manages	Physical protection, personnel screening, contingency planning, and supply chain	NIST SP 800-53
PCI DSS	Shared responsibility for the cardholder data environment	Privileged access, least privilege, logging, and monitoring for accounts the suite manages	Network controls, malware protection, and physical access	PCI DSS
HIPAA Security Rule	Covered entity and business associate duties	Administrative and technical access, audit, and Incident Response records in the product	Physical safeguards, workforce designation, and the covered-entity determination	HIPAA
GDPR and California privacy	Controller and processor; accountability and reasonable security	Access control, audit, records of processing support, and the Assessment Binder	Lawful basis, data-subject response, and the controller role	GDPR, California privacy
SOC 2	Service organization vs complementary user-entity controls	Trust-services work the suite performs: access, logging, change evidence, and Incident Response records	User-entity controls, facilities, and the service auditor's opinion	SOC 2
HITRUST	Assessed entity and inherited controls across 19 domains	Access, logging, and incident records the suite creates	Organizational domains HITRUST leaves with the assessed entity	HITRUST
ISO/IEC 27001	Annex A themes; organization remains the certified party	Access, cryptography use, operations logging, and Incident Response records in the product	The Information Security Management System and the certification body decision	ISO/IEC 27001

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Framework	What they call the split	What AIC supplies	What stays with you	Page
IEC 62443	Zones, conduits, and foundational requirements	Privileged access, Jump, Privileged User Management, and configuration compliance for engineering access	Plant safety, physical zones, and the asset-owner role	IEC 62443
NERC CIP	Responsible entity for CIP-002 through CIP-015	Privileged Identity Management for shared and default accounts, audit, and configuration compliance	Bulk Electric System designation and the responsible-entity role	NERC CIP
Australian Essential Eight and NIS2	Maturity strategies and Article 21 measures	Patch evidence support, privileged access, and logging the suite produces	Strategy level, national filing, and the essential-entity determination	Essential Eight, NIS2

CMMC external service providers

32 CFR Part 170 Table 4 to section 170.19(c)(2)(i) is the CMMC scoping table for External Service Providers. An ESP is an outside party that provides information technology or cybersecurity services on your behalf, and CUI or Security Protection Data (SPD) is on that party's assets. A CSP provides cloud computing, as defined in NIST SP 800-145. When CUI is in a FedRAMP or GCC cloud, 48 CFR 252.204-7012 and FedRAMP Moderate (or equivalent) apply to that CSP.

- AIC is not the CSP in any of the three hosting models.
- On premises: CUI and SPD stay on your assets. You run AIC. AIC is not the ESP.
- Commercial IaaS: you exclusively control the enclave, the cryptography, and access. You do not use the cloud provider's managed services. You run pre-installed AIC software. AIC is not the ESP.
- FedRAMP or GCC: AIC is an authorized application under the cloud provider's authority. The cloud provider remains the CSP. Shared duties are in the CRM next to the provider's CRM.
- If an MSP operates the environment and CUI or SPD is on that MSP's assets, that MSP may be the ESP.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Frequently Asked Questions

Where does regulated data live?
On premises: in your site. Commercial IaaS: in the enclave you control on that infrastructure. FedRAMP or GCC: on the authorized cloud. That includes CUI, FCI, cardholder data, protected health information, personal data, and operational technology access records. AIC is not a separate cloud that replaces the hosting you chose.

Who holds the encryption keys?
You do. In every model, you exclusively control cryptography unless you delegate it. Keys live in software, in an HSM, or in a key service you own. AIC encrypts with the keys you designate. AIC does not take ownership of your keys. An MSP holds keys only if you delegate that duty. In commercial IaaS you do not use the cloud provider's key service.

Is AIC FedRAMP authorized?
No. In model 3, the cloud provider holds the FedRAMP or GCC authorization. AIC operates under that authority as an authorized application. Models 1 and 2 do not use a FedRAMP or GCC authorization.

If we use an MSP, is AIC the MSP?
No. AIC supports MSPs. Your MSP may operate the environment inside your boundary. That MSP may be the ESP. AIC remains the software you run, or the authorized application on a FedRAMP or GCC cloud, as you chose.

Is CMMC the only program this covers?
No. CMMC is one regulatory framework. The three hosting models support FedRAMP, GCC, NIST SP 800-53, NIST SP 800-171, NIST SP 800-172, PCI DSS, GDPR, California privacy, ISO/IEC 27001, SOC 2, HITRUST, HIPAA, IEC 62443, NERC CIP, Essential Eight, NIS2, and most other GRC frameworks. See Frameworks.

Does a PCI DSS, HIPAA, or SOC 2 assessor use Table 4?
No. Table 4 is the CMMC ESP and CSP table. Those other programs still require a written split of duties. For PCI DSS it is the cardholder data environment. For HIPAA it is covered-entity and business-associate work. For SOC 2 it is service-organization and user-entity controls. The CRM on this page is that split.

If we are the controller under GDPR, is AIC the processor?
In on-premises and commercial IaaS hosting, you run the software. AIC does not host your data and is not your processor. In FedRAMP or GCC hosting, AIC is an authorized application under the cloud provider's authority. Your contract with that provider, and the CRM, name who processes personal data.

Do operational technology programs change the hosting models?
No. IEC 62443 and NERC CIP use the same three models. You still own the plant, the

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Bulk Electric System designation, and safety. AIC supplies privileged access, Jump, configuration compliance, and the evidence those programs read.

Do we still need a CRM in models 1 and 2?
Yes. In models 1 and 2, you run AIC, and AIC is not the ESP or the CSP. The CRM still names who owns the site or the IaaS, the application, the keys, the workforce, Incident Response, and the assessment.

Does AIC replace our cloud provider?
No. AIC supports cloud providers on GCC and FedRAMP offerings, and supports commercial IaaS when you want a customer-controlled enclave. The provider stays the infrastructure or the authorized cloud. AIC adds the cybersecurity and GRC layer.

What is different about commercial IaaS?
The commercial cloud is not FedRAMP or GCC. You use it as infrastructure only. You do not consume that provider's managed services. You build the secure enclave on STIG-hardened virtual machines, with a public and private network you define. You exclusively control the environment, the cryptography, and access. AIC is pre-installed software that you run.

Related Pages

- Frameworks
- Capabilities
- CMMC
- NIST SP 800-53
- PCI DSS
- HIPAA
- GDPR
- SOC 2
- ISO/IEC 27001
- IEC 62443
- NERC CIP
- Security

Products and Contact

- AIC Enterprise Privilege Suite™

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

- AIC CMMC Complete™
- Frameworks
- Pricing
- Contact

Auditor and Readiness Resources

C3PAO Partners and Auditor Resources includes walkthrough exercises for reviewing responsibility boundaries and supporting evidence.

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.