Analog Informatics™ Corporation

C3PAO Partners and Auditor Resources

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

analoginfo.com

Revised 29 October 2026

View this resource online

Security First. Continuous Compliance. Evidence from Daily Operations.

Secure systems, controlled privileges, current records, and accountable operators are the foundation. Compliance evidence should come from that work every day, rather than from a scramble before an assessment.

AIC Enterprise Privilege Suite™ and AIC CMMC Complete™ connect security operations with the records an assessor needs to examine. Current state, control history, privileged activity, and supporting documents help explain what is operating, who owns it, and what changed between reviews.

Resources for All Auditors

These resources serve C3PAOs, independent auditors, internal audit teams, and assessment organizations working across the frameworks AIC supports. Security operations, evidence traceability, and documented responsibility boundaries matter across SOC 2, ISO/IEC 27001, PCI DSS, HIPAA, NIST-based programs, and CMMC.

Some assessment organizations provide services across several standards. C3PAO authorization relates specifically to CMMC; each firm's other audit, attestation, or certification services depend on its qualifications and service scope. SOC 2 examinations and reports are performed by licensed CPA firms. Directory profiles will identify each organization's verified services separately.

Use the tutorials below with the applicable framework, assessment objectives, and evidence period. The same operational record may support several reviews, while each auditor evaluates its relevance and sufficiency for the engagement.

Auditor tools for all supported frameworks · Supported frameworks · SOC 2 · ISO/IEC 27001

Find an independent C3PAO · Learn the evidence workflow · Request an assessor walkthrough

Readiness Practitioners and Independent Auditors

We support both the professionals who help an organization improve security and prepare for an audit, and the independent professionals who examine its controls and evidence. These are separate responsibilities, including when an organization offers both practices.

Readiness practitioners help customers define scope, implement security controls, address findings, document procedures, and organize evidence. Independent auditors examine the implementation and supporting records, perform their assessment work, and reach their own conclusions.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Engagement role	Product access and responsibility	Audit authority
Readiness practitioner	Customer-authorized permissions for assigned preparation, configuration, remediation, and documentation work.	Practitioner access does not authorize audit sign-off or certification decisions.
Independent auditor or assessor	Read-only access to the evidence and Assessment Binder records authorized for the engagement.	Audit conclusions and sign-off remain with the appropriately qualified, independent assessment professional or organization.
Customer administrator	Assigns scoped access for the engagement and manages operational permissions.	Assigning a product role does not grant professional authority to issue an audit opinion or certificate.

Read-only evidence access keeps the assessment role separate from the ability to change the implementation or its supporting records. Preparation permissions do not confer audit approval authority. A readiness review, completed remediation task, or prepared evidence package is distinct from an independent audit conclusion.

Where a firm operates separate readiness and audit practices, the engagement must satisfy the applicable framework's independence and conflict-of-interest requirements. Separate accounts, permissions, or practice names alone do not establish independence. Review prior consulting, implementation, and product services before appointing an assessor.

Readiness and implementation services · Independent C3PAO assessment · Auditor tools

Professional Roles by Program

Preparation, assessment, and formal issuance are different responsibilities. A person's credential, a firm's authorization, and the role assigned for a customer engagement must be checked separately. A person may hold several credentials; that does not remove the independence requirements for the engagement.

CMMC readiness and assessment roles

Designation	Who holds it	Role
Registered Practitioner (RP) or Registered Practitioner Advanced (RPA)	Individual	Registered readiness and implementation practitioner. These are registration designations, not assessor certifications.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Designation	Who holds it	Role
Registered Practitioner Organization (RPO)	Organization	Registered provider of readiness and implementation services. Registration does not authorize certification assessments.
CMMC Certified Professional (CCP)	Individual	Certified professional credential; does not authorize final assessment determinations.
CMMC Certified Assessor (CCA) or Lead CMMC Certified Assessor (Lead CCA)	Individual	Performs certification assessment work through a C3PAO, within the individual's qualified role.
CMMC Third-Party Assessment Organization (C3PAO)	Organization	Authorized or accredited organization conducting Level 2 certification assessments.
Authorized Certifying Official	Designated C3PAO official	Signs and issues the Certificate of CMMC Status on behalf of the C3PAO.

Verify registrations, credentials, and organization status through the Cyber AB Marketplace. See the Cyber AB's consulting roles, assessment roles, and CMMC Assessment Process.

Roles across other supported frameworks

Program	Readiness and implementation	Independent review or formal assurance
SOC 2	SOC 2 readiness consultant or adviser. List any separately verified professional credentials.	Licensed CPA firm performing a SOC 2 examination and issuing a report. A readiness service is not a SOC 2 report.
ISO/IEC 27001	ISMS implementation consultant; identify the issuer of any verified Lead Implementer credential.	ISMS auditor or Lead Auditor, with the credential issuer identified; certification is issued by a certification body. Verify the body's accreditation and scope separately.
PCI DSS	PCI DSS readiness consultant; identify any verified QSA qualification separately.	Qualified Security Assessor (QSA) Company and its qualified QSA Employees, where the assessment calls for a QSA.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Program	Readiness and implementation	Independent review or formal assurance
HITRUST	HITRUST readiness practitioner; identify a verified Certified CSF Practitioner (CCSFP) credential where held.	HITRUST Authorized External Assessor organization. Individual CCSFP and Certified HITRUST Quality Professional (CHQP) credentials identify practitioner and quality-review qualifications.
FedRAMP	FedRAMP adviser or readiness consultant.	FedRAMP Recognized independent assessment service; legacy materials use Third-Party Assessment Organization (3PAO). Verify recognition for the applicable program path. This is distinct from a CMMC C3PAO.
HIPAA	HIPAA privacy or security adviser.	Internal or external evaluator under the applicable requirements. HHS does not recognize private Security Rule certifications.
NIST-based programs	Security implementation practitioner with experience in the relevant NIST publications.	Security assessor under the applicable agency, contract, or assurance program. NIST SP 800-171 itself does not confer a NIST-issued consultant or auditor certification.
GDPR	Privacy adviser, with individual credentials and their issuers identified separately.	Independent reviewer; an accredited certification body is a separate role under an applicable GDPR certification mechanism.
NIS2	Cybersecurity readiness practitioner.	Independent reviewer or auditor under the applicable national requirements; identify the jurisdiction and supervisory authority.
NERC CIP	NERC CIP readiness or implementation consultant.	The relevant Compliance Enforcement Authority conducts regulatory compliance monitoring; a private readiness review is a separate service.
ISA/IEC 62443	Industrial cybersecurity practitioner; identify the exact ISA certificate or other verified credential.	Assessor or certification body under the named conformity-assessment scheme. A person's training certificate does not confer certification-body authority.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Official program references: AICPA SOC services, ISO/IEC 27001, IRCA ISMS auditor certification, PCI SSC QSAs, HITRUST Assessment Handbook, FedRAMP assessment services, HHS Security Rule evaluations, NIST SP 800-171 primer, EDPB certification-body guidance, NIS2, NERC compliance, ISA certificates, and ISASecure certification bodies.

Credentials and Product Permissions

Directory credentials describe professional qualifications. Product permissions control access for the engagement. RP, RPA, RPO, CCP, CCA, QSA, or any other directory designation must not automatically grant product administration or audit approval rights.

Readiness access supports the preparation work the customer authorizes. Auditor access is read-only to the authorized evidence. Independent findings, reports, and certificate issuance remain with the appropriate professionals and organizations under the program's rules. The customer's own affirmation or readiness acceptance is separate from an independent audit opinion or certification decision.

Resources for Assessment Teams

Resource	What you will find
Shared responsibility and hosting Q&A	Public answers about deployment models, cloud and service-provider roles, and responsibility boundaries.
Assessment evidence	Evidence preparation and the connection between requirements and supporting records.
Auditor tools	Product resources for reviewing security activity and evidence.
Supported frameworks	Framework-specific resources for auditors and assessment teams across the standards AIC supports.
SOC 2	Security controls and supporting evidence relevant to SOC 2 examinations.
ISO/IEC 27001	Security management and evidence resources for ISO/IEC 27001 reviews.
Requirements mapping	The relationship between product capabilities and CMMC requirements.
Evaluation guide	A structured starting point for evaluating the products.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Resource	What you will find
Product screenshots	Product screens for orientation before a walkthrough.
Continuous compliance	Security operations and evidence maintained between assessments.

Assessor Tutorials

These exercises use sample data in a demonstration environment. Request a walkthrough to work through them with AIC. Customer evidence is shared separately through the customer's approved process.

1. Establish scope and responsibility

1. Identify the deployment model, assessment boundary, selected requirements, and systems included in the demonstration.
2. Use separate readiness-practitioner and read-only auditor accounts. Confirm that the auditor can review the authorized evidence without changing it, and that preparation permissions do not grant audit sign-off authority.
3. Use the public shared-responsibility Q&A to distinguish AIC software from the cloud provider and any operator or MSP.
4. For a customer engagement, obtain the engagement-specific Customer Responsibility Matrix through the authorized contact. Confirm who operates each relevant control and who supplies its evidence.
5. Record excluded systems and dependencies. Product coverage and assessment scope must be evaluated together.

Review outcome: a defined boundary, named evidence owners, and a list of external dependencies.

2. Follow a requirement to its evidence

1. Select a requirement within the demonstrated product coverage.
2. Review its current state and coverage information.
3. Locate its supporting artifacts in the Assessment Binder. Identify the source system, collection time, responsible person, and period each artifact supports.
4. Identify supporting interviews and tests needed to evaluate the requirement. Record missing or unclear evidence for the customer to resolve.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Review outcome: a traceable relationship between the requirement, the implementation, and the supporting records.

3. Review operation over time

1. Review the available control state history for the selected requirement.
2. Examine a change or exception and the records explaining what happened.
3. Compare the current state with earlier records and the documented response. Identify gaps in collection or coverage.
4. Agree the evidence period and sampling approach with the assessment team.

Review outcome: evidence of operation across time, including exceptions, rather than a single favorable screenshot.

4. Trace privileged activity

1. Select a sample privileged activity from the demonstration's audit records.
2. Identify the account, actor, target, and time from the available records.
3. Review the associated session recording where that access path is recorded.
4. Compare the activity with the applicable access policy and supporting approval records supplied by the operator.

Review outcome: a reviewable trail from privileged access to the activity performed.

5. Prepare the evidence handoff

1. Agree the evidence request list, authorized recipients, review period, and secure transfer method.
2. Organize the supporting artifacts by requirement in the Assessment Binder. Distinguish product-generated records from customer-supplied policies, interviews, and other evidence.
3. Check timestamps, readable labels, source references, and unresolved requests before handoff.
4. Confirm receipt and track follow-up requests with the responsible owner. Preserve the original records under the customer's retention and access rules.

Review outcome: an organized evidence package with clear ownership and fewer repeated requests for the same information.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

What the Products Provide

Evidence area	Current availability
Current State Compliance, control coverage, and control state history	Available now for systems and paths managed by the kit; wider scope is planned or remains with the organization.
Assessment Binder and POA&M entries	Available now; the organization supplies records for responsibilities outside product coverage.
Session recording and audit records	Available now for the supported access paths in use.

Use the walkthrough to confirm coverage for the customer's actual deployment and product version.

Reliable Evidence Starts Before the Assessment

Agree a consistent evidence format early: requirement reference, source, collection time, coverage period, responsible owner, and related exception or remediation record. Keep records current as systems and responsibilities change. Restrict access to the people authorized to review them.

A standardized evidence package can reduce time spent locating, renaming, and explaining artifacts. Ask the C3PAO how evidence quality and readiness affect its proposed effort and fee. The C3PAO sets its scope, sampling, and commercial terms independently.

Independent Assessment Relationships

Auditors across all supported frameworks retain responsibility for their own professional judgments, evidence requirements, and applicable independence obligations.

C3PAOs participate here as independent assessment organizations. A listing identifies a contact and available assessment services; it does not represent a product recommendation or endorsement.

Assessment teams can provide factual feedback about evidence organization, traceability, and review effort within their professional obligations. Assessment conclusions remain their own. Product education and directory participation must preserve the C3PAO's impartiality and conflict-of-interest requirements.

Copyright © 2026 Analog Informatics Corporation. All rights reserved.

Find a C3PAO

Check Back Soon

Use the Cyber AB Marketplace to check an organization's current authorization or accreditation before engaging it. Discuss scope, relevant experience, availability, evidence handling, independence, and fees directly with the assessment organization.

Ask about C3PAO introductions

Join the C3PAO Directory

Contact AIC to discuss an assessor walkthrough or a directory listing. Provide your organization's name, Cyber AB Marketplace profile, assessment contact, service coverage, website, and permission to publish the listing. Identify whether you offer readiness, independent assessment, or both, and provide the relevant individual credentials, organization authorizations, issuing bodies, and current verification records. Include any restrictions your impartiality policy places on directory participation or product education.

Contact AIC

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

Copyright © 2026 Analog Informatics Corporation. All rights reserved.