Security & Trust Overview

Last Modified on 07/16/2026 11:53 am EDT

Info-Tech takes a data-centric approach to securing CIO Analytics: member data is encrypted in transit and at rest and isolated within Info-Tech's secured environment. The product is developed and operated under Info-Tech's **SOC 2 Type II** and **ISO/IEC 27001:2022**–certified processes, within the AWS and Azure infrastructure where member data is processed and stored.

Download PDF version of this page

Beta release
CIO Analytics is currently in beta release to Info-Tech Advisory members. The security controls described here are in place today; certifications and roadmap items are labeled as such.

In this document

Certifications at a glance

AICPA SOC 2® TYPE II

● **Attested**

Independently examined. Full report to members under NDA.

ISO/IEC 27001:2022

● **Certified**

Current revision. Certificate available on request.

CYBER ESSENTIALS

● **Certified**

NCSC scheme. Baseline technical controls.

ISO/IEC 42001:2023

◐ **In progress**

AI management systems. Certification underway.

01 Certifications & Frameworks

CIO Analytics was built and is operated using Info-Tech Research Group's independently certified processes. Info-Tech has maintained its core certifications for over five years. Beyond the certifications above, our controls align with established security frameworks:

NIST SP 800-171 Rev. 3	Our controls are mapped to this framework for protecting Controlled Unclassified Information.

Our SOC 2 Type II examination covers the Security Trust Services Criterion.

02 Architecture & Data Flow

1. Member configures the connection to their ITSM platform through the **cioanalytics.ai** site (AWS, US West).
2. **Fivetran**, running in its own Azure environment (East US 2), connects to the member's ITSM and moves data into the Microsoft **Fabric** lakehouse in a secure Azure tenant (US West) over **TLS 1.3**.
3. Data is normalized entirely within the Fabric environment.
4. **Cube Cloud** provides the semantic layer (AWS, US East) before results are served back through the same site.

> **At no point does member data leave the United States.**
> All storage and processing remains in US AWS & Azure regions.

Supported ITSM platforms

- Freshservice
- ManageEngine ServiceDesk Plus
- ServiceNow
- TeamDynamix
- HaloITSM
- ZenDesk
- Solarwinds
- SysAid

Additional platforms are evaluated on member demand.

Sub-processors

Amazon Web Services	Web application & serving tier	US: US West
Microsoft Azure / Fabric	Data lakehouse & processing	US: US West
Fivetran	ITSM connectivity; holds connection credentials	US: Azure East US 2
Cube Cloud	Semantic layer prior to serving	US: AWS US East

03 Data Residency

Where is our data stored?

All member data is stored and processed within the United States across Info-Tech's AWS (US West) and Azure (US West) environments, with the semantic layer in AWS US East. Data does not leave the United States.

Where is data accessed from?

Member data is stored and processed within the United States and does not leave US-based infrastructure. Access is limited to authorized Info-Tech personnel. This includes specialized support staff based in Canada, and research analysts who may view a member's dashboards — the product's presentation layer rather than the underlying data store — from locations outside the United States and Canada in order to provide analysis to that member. All such access is role-based, least-privilege, and logged.

04 Encryption

In transit?

Connectivity to and from member ITSM platforms and the Fabric environment uses **TLS 1.3**.

At rest?

All member data is encrypted at rest using **AES-256**.

Key management?

Encryption keys are managed through dedicated key management services: Azure Key Vault, AWS KMS, and Fivetran's key management. Customer-managed keys (BYOK) are not offered in beta.

05 Credential Handling

How are our ITSM credentials handled?

Members supply their own ITSM credentials during setup. **Info-Tech does not persist member credentials** in its environment; they are passed to and held within Fivetran's audited environment solely for the configured data connection.

06 Ownership & Retention

Who owns the data?

Members retain **full ownership** of their data at all times.

Retention & deletion?

Data is retained for the duration of the member relationship. On termination or request, it is deleted across **all processing tiers** — lakehouse and semantic layer — within **two weeks (14 calendar days)**.

Deletion on request mid-contract?

Members may request deletion of their data **at any time**, during or at the end of the contract.

07 Data Handling & Isolation

What ITSM data is ingested?

CIO Analytics ingests a defined set of data points from each supported ITSM platform, not an unrestricted full export. Within that set, data is ingested as-is (full fidelity) and protected by the encryption, access, and isolation controls described here. CIO Analytics requires only read-only access to member ITSM systems and does not write to or modify them; where a platform's API does not support a read-only credential scope, access remains limited to read operations by CIO Analytics' configuration.

How is our data isolated from other members?

Each member's data is logically separated within the Fabric environment, with access controls enforcing separation between members.

08 AI Governance

How is AI governed?

CIO Analytics uses generative AI to produce insights from member data, served from the Azure tenant described above using Azure AI services. Member data is not sent to external AI providers and is **never**

used to train large language models. The underlying models may change over time as more effective ones become available, and remain served from the same Azure tenant. AI governance is managed under Info-Tech's **ISO/IEC 42001:2023** program (certification in progress), with models reviewed on an ongoing basis to maintain quality and governance.

09 Access, Resilience & Incident Response

How is access controlled?

Info-Tech staff access to member data is role-based, least-privilege, and logged. Member sign-in supports SSO, with MFA enforced through the member's own identity provider.

Availability & recovery

As CIO Analytics is in beta, formal uptime SLAs and recovery objectives are not yet published. Runs on enterprise cloud infrastructure (AWS, Azure) with regular backups; commitments defined approaching GA.

Incident response

Documented incident response process. Affected members are notified within **72 hours** of confirming a security incident affecting member data.

Request the full security package
Info-Tech's complete documentation, including the SOC 2 Type II report and ISO/IEC 27001 certificate, is available to members under NDA. Security contact: security@infotech.com.