

COMPLIANCE CAPABILITY REPORT

Nucleus One and SOX: Compliance Capability Report



BUILT ON GOOGLE CLOUD

Independent certifications of the Google Cloud infrastructure Nucleus One runs on. Reports available through Google Cloud's Compliance Reports Manager; the public SOC 3 summary and the ISO 27001 certificate require no account.

How Nucleus One's enforced approvals, document event history, revision integrity, and access controls support your organization's internal controls over financial reporting.

Issued September 2026 · Prepared by Ademero, Inc. for customer compliance and IT review

Executive summary

Sarbanes-Oxley compliance attaches to a company's internal controls over financial reporting (ICFR); software provides the control capabilities and evidence those controls are built on. Nucleus One provides both in depth: approvals that enforce themselves, a complete who-did-what event history on every document, version history that cannot be rewritten in normal application use, deliberate access control, and organization-enforced multi-factor authentication — on Google Cloud infrastructure independently attested to SOC 2 Type II and SOC 1 Type II and certified to ISO 27001. The table below maps each SOX control objective to the capability that serves it and the evidence it produces for control testing.

Capability mapping

SOX CONTROL OBJECTIVE	NUCLEUS ONE CAPABILITY	EVIDENCE PRODUCED
Authorization — documents approved before they take effect	Approval Processes with group approvals requiring any, all, or a majority of assignees; required fields block approval of incomplete records; block re-entry prevents decided items from re-entering approval	Every approve/decline recorded with process name, step, participants, and timestamp
Change management and audit evidence	Document events: twelve event types (revisions, field changes, name changes, folder moves, approval actions, signature events, and more) with actor, timestamp, and before/after detail	Per-document event log plus a project-wide, filterable Events feed
Data integrity — originals preserved, changes visible	Full revision history retained with author and timestamp; restoring an earlier revision creates a new revision rather than overwriting history	Complete version lineage with visual comparison between revisions
Logical access (ITGC)	Organization and project roles (administrator, project manager, stakeholder, read-only); per-area access levels (Everything / Direct assignments / Nothing); folder sharing with inheritance; project groups	Membership and access configuration reviewable per project
Segregation of duties (ITGC)	Approvals assignable to users or groups distinct from submitters; project setting disallows content removal by non-manager members	Process and project configuration demonstrating the separation
Access security (ITGC)	Organization-enforced multi-factor authentication (TOTP) for all members; scoped API keys	MFA enforcement visible in organization Security Settings

The certification layer: infrastructure attestations and application controls

Nucleus One runs entirely on Google Cloud (App Engine, Cloud Firestore, Cloud Storage). Every layer beneath the application — data centers, physical security, network, storage durability, encryption at rest and in transit, and operational controls — is covered by Google Cloud's independent SOC 2 Type II and SOC 1 Type II attestations and ISO 27001 certification. These reports are available directly through Google Cloud's Compliance Reports Manager (cloud.google.com/security/compliance/compliance-reports-manager); the public SOC 3 summary and the ISO 27001 certificate are available there without a Google account. This shared-responsibility structure — infrastructure attestations from the cloud provider, application controls from the software vendor — is the same model AWS- and Azure-hosted software uses. At the application layer, Nucleus One adds organization-enforced multi-factor authentication (TOTP), role- and area-scoped access control, enforced multi-party approvals, complete document event history, and revision integrity, all served exclusively over HTTPS with strict transport security.

Scope of this report — This report describes product capabilities and the attestations of the underlying infrastructure. It is not a certification of regulatory compliance, which attaches to your organization's processes and controls; no software product can be certified as SOX-compliant. Statements reflect the product as of the issue date above. This document is not legal or audit advice.