



**InsightVector**  
CONSULTING

Project delivery, controlled.

## CLIENT SECURITY BRIEF

# Acnos Security and Platform

A practical guide to the platform boundary, shared responsibilities, access and data controls, release discipline, support, and buyer diligence.

|                 |                                                                                                                      |
|-----------------|----------------------------------------------------------------------------------------------------------------------|
| <b>FOR</b>      | IT, security, procurement, privacy, legal, operations, and executive reviewers                                       |
| <b>USE</b>      | Prepare platform, licensing, access, data, integration, support, and incident questions for a proposed Acnos release |
| <b>POSITION</b> | Acnos is configured and governed within the client's approved Zoho environment under a defined service scope         |

# A Clear Starting Position

Acnos by InsightVector is a service-backed project delivery and project-to-cash operating system implemented on the Zoho platform.



## Delivery model

Configured and governed within the client's approved Zoho environment; not positioned as independent InsightVector-hosted SaaS.

## Licensing

Client Zoho subscriptions are separate unless the executed agreement expressly includes them.

## Data

Client data ownership, access, export, retention, and deletion responsibilities are defined by contract and applicable Zoho terms.

## Access

Named access, least privilege, controlled administration, and client-approved role design are baseline Acnos controls.

## Security boundary

Zoho operates the underlying platform; the client governs users, subscriptions, data, and policies; InsightVector governs contracted configuration and support work.

## Verification

Capabilities vary by Zoho product, edition, region, and configuration. The release manifest and solution design identify the exact scope.

### IMPORTANT

This brief is not a certification, penetration-test report, data-processing agreement, security addendum, or substitute for the client's own vendor-risk review.

# What Acnos Is - and Is Not

The strongest security conversation begins with a precise operating model, defined authority, and claims that stay inside the executed scope.

**A service-backed operating system**

Acnos combines configured Zoho capabilities with solution design, project-to-cash controls, release evidence, and contracted support.

**A client-environment implementation**

The solution operates inside the approved Zoho organization and products selected for the client release.

**Not independent InsightVector-hosted SaaS**

Under the current delivery model, Acnos is not positioned as a separate platform owned or hosted by InsightVector.

**Not universal product equivalence**

Do not assume every Zoho product, edition, region, portal, API, export, or integration provides the same control set.

**Not a specialist-system replacement**

Acnos is not a replacement for Procore, Primavera P6, Autodesk Construction Cloud, or specialist field systems.

**Not unlimited administration authority**

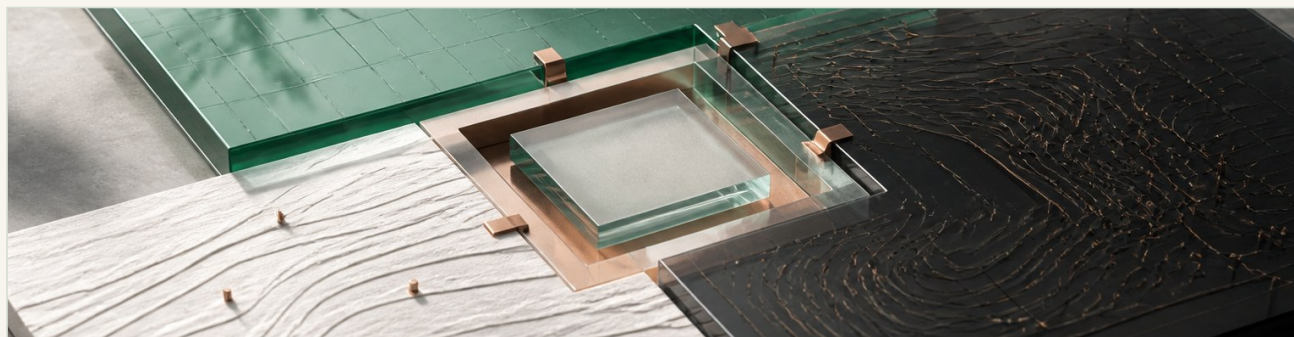
InsightVector does not administer users, access data, or change the client environment outside contracted and approved authority.

## Before a client relies on any platform feature or control

| Confirm                                    | Evidence to capture                                       |
|--------------------------------------------|-----------------------------------------------------------|
| Exact products and editions                | Product and license schedule tied to the proposed release |
| Client organization and data center        | Environment record and platform-region confirmation       |
| Users, portals, roles, and connections     | Approved access design and integration inventory          |
| Contracted configuration and support scope | Release manifest, solution design, and support schedule   |

# The Shared Responsibility Model

Security and reliability depend on coordinated controls across the platform provider, client environment, and InsightVector delivery scope.



| Zoho platform                          | Client environment                       | InsightVector / Acnos                   |
|----------------------------------------|------------------------------------------|-----------------------------------------|
| Hosts and operates subscribed services | Owns subscriptions and client data       | Designs contracted configuration        |
| Platform security and availability     | Approves users, roles, and policies      | Governs build, test, and change         |
| Product-level safeguards and terms     | Accepts processes and operating controls | Supports only within approved authority |

## CONTROLLED BOUNDARY

Client credentials, tokens, and secrets are not stored in Acnos deployment-control records.

## Control ownership at the interface

| Control area               | Primary owner                 | Acnos / client interface                                                                 |
|----------------------------|-------------------------------|------------------------------------------------------------------------------------------|
| Platform operations        | Zoho                          | Client verifies subscribed services, terms, region, and required assurances.             |
| Subscriptions / editions   | Client                        | InsightVector identifies required capabilities; client approves procurement.             |
| Users and identity         | Client                        | InsightVector proposes roles and least-privilege design within approved authority.       |
| Client data classification | Client                        | InsightVector configures agreed fields, workflows, and evidence handling.                |
| Acnos solution design      | InsightVector                 | Client approves scope, process, permissions, and acceptance criteria.                    |
| Configuration change       | InsightVector within contract | Client authorizes; InsightVector tests, evidences, and releases approved changes.        |
| Third-party connections    | Client + platform owners      | InsightVector documents approved dependencies and test results.                          |
| Business continuity        | Shared                        | Platform, client operations, and contracted support obligations are assessed separately. |

# Identity, Access, and Data Handling

The client remains the authority for who may access its environment and what data may be processed.

| Control                        | Expected posture                                                                                                     | Owner                                     |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------|-------------------------------------------|
| <b>Named access</b>            | Use named accounts; avoid shared administrative identities; document service accounts where unavoidable.             | Client                                    |
| <b>Least privilege</b>         | Map job responsibilities to roles, profiles, field visibility, and approval authority.                               | Client approves;<br>InsightVector designs |
| <b>MFA</b>                     | Zoho Accounts supports MFA modes. Enforce according to client policy and verify portal-user requirements separately. | Client                                    |
| <b>SSO</b>                     | Confirm SAML/SSO availability and policy controls for selected subscriptions and user population.                    | Client + Zoho                             |
| <b>Admin access</b>            | Time-bound, purpose-limited, and approved administration; remove access when work concludes.                         | Client + InsightVector                    |
| <b>Joiner / mover / leaver</b> | Define who requests, approves, provisions, reviews, and revokes access.                                              | Client                                    |
| <b>Access review</b>           | Review privileged and business-critical roles on a risk-based cadence and after material change.                     | Client                                    |
| <b>Evidence access</b>         | Use approved repositories and links; restrict sensitive records; avoid unnecessary duplication.                      | Client + InsightVector                    |

## Connections and secrets

### Keep secrets out of ordinary records

Client credentials, passwords, API tokens, and secrets are not stored in Acnos CRM fields, ordinary documents, logs, screenshots, or source code.

### Use approved connection mechanisms

Connections are created only through platform-approved mechanisms and after owner authorization.

### Retain non-secret evidence

Deployment records may retain environment references, version evidence, test results, and ownership metadata.

### Review support artifacts

Logs and support evidence are checked for sensitive content before sharing or retention.

# What Zoho Publishes About the Platform

The positions below summarize official Zoho material reviewed on August 21, 2026. They describe the platform provider, not an independent Acnos certification.

| Area                      | Published position                                                                                                                     | Client verification                                                    |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| <b>Transport security</b> | Zoho documents TLS for data traveling between users and Zoho servers and for supported server-to-server connections.                   | Confirm integration endpoints and product behavior.                    |
| <b>Encryption at rest</b> | Zoho describes encryption at rest based on data sensitivity and product implementation; product documentation may provide more detail. | Confirm exact services and data types.                                 |
| <b>MFA</b>                | Zoho Accounts documents multiple MFA modes and organization policy behavior.                                                           | Define enforcement and recovery controls.                              |
| <b>Data center</b>        | Zoho states that account data-center assignment is associated with the country selected at signup.                                     | Record actual data center and cross-region requirements.               |
| <b>Assurance</b>          | Zoho trust and compliance pages list ISO 27001, ISO 27017, ISO 27018, and SOC 2 Type II, among other programs.                         | Verify certificate scope, entity, product applicability, and validity. |
| <b>Export / deletion</b>  | Zoho privacy material states that export and deletion options are provided within each service; behavior and formats vary.             | Test required exports and retention workflows.                         |
| <b>DPA</b>                | Zoho publishes a process for organization administrators to request or execute a data processing addendum.                             | Client legal/privacy owner determines need.                            |
| <b>API limits</b>         | Zoho CRM terms state that API usage limits may apply and can affect uninterrupted service.                                             | Design for edition limits, retries, and partial failure.               |

## ASSURANCE RULE

Do not treat a platform-level certification as proof that a specific Acnos configuration, client process, or integration is compliant. Scope and configuration must be assessed together.

# Acnos Configuration and Release Controls

InsightVector's service controls govern how the contracted operating model is designed, changed, tested, accepted, and transitioned.



| Control                       | Minimum practice                                                                                            | Evidence                              |
|-------------------------------|-------------------------------------------------------------------------------------------------------------|---------------------------------------|
| <b>Approved scope</b>         | Release manifest identifies in-scope capabilities, products, owners, dependencies, and prohibited variance. | Approved manifest                     |
| <b>Environment readiness</b>  | Verify client ownership, subscriptions, roles, connections, templates, and security prerequisites.          | Readiness record                      |
| <b>Configuration control</b>  | Changes are versioned, attributable, and tied to approved requirements or change requests.                  | Configuration register                |
| <b>Migration</b>              | Approved batches reconcile counts, keys, relationships, status, and monetary totals.                        | Migration and reconciliation evidence |
| <b>Testing</b>                | Cover happy path, blocked path, permissions, duplicates, replay, partial failure, analytics, and recovery.  | Test results and defects              |
| <b>UAT</b>                    | Authorized business roles validate the process and evidence against acceptance criteria.                    | UAT decision                          |
| <b>Cutover</b>                | Activate only approved components; run smoke tests; preserve rollback posture.                              | Cutover record                        |
| <b>Operational acceptance</b> | Ownership, support, access, and residual risk are accepted before transition.                               | Acceptance / handoff                  |

# Secure Automation Requires Operating Discipline

Automation is controlled through ownership, versioning, bounded authority, exception evidence, reconciliation, and human review.

|                                                                                                                                        |                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Registry and ownership</b><br><br>Maintain an automation registry with owner, version, trigger, dependencies, and business purpose. | <b>Duplicate prevention</b><br><br>Use correlation identifiers and duplicate-prevention controls for transactions that may retry or replay.    |
| <b>Safe logging</b><br><br>Log material outcomes and exceptions without exposing secrets or unnecessary personal data.                 | <b>Controlled failure</b><br><br>Route failed or partial transactions to controlled retry, reconciliation, or human review.                    |
| <b>Proportionate watchdogs</b><br><br>Use watchdog and reconciliation controls proportionate to business and financial impact.         | <b>Bounded authority</b><br><br>Do not grant automations uncontrolled authority for contracts, invoices, payments, or external communications. |

## Reliability design test

| Question                         | Evidence expected                                                                        |
|----------------------------------|------------------------------------------------------------------------------------------|
| What triggers the automation?    | Approved event, input state, eligibility rule, and business purpose                      |
| How is repeat execution handled? | Correlation key, duplicate rule, idempotent behavior, or reconciliation path             |
| What happens on partial failure? | Exception state, controlled retry, rollback or recovery, and accountable owner           |
| What authority is prohibited?    | Documented limits for financial, contractual, access, and external communication actions |
| How is health monitored?         | Material outcome logs, alert thresholds, watchdog evidence, and periodic reconciliation  |

DESIGN PRINCIPLE

Reliable automation is not defined by a successful happy path. It is defined by how safely the process detects, contains, explains, and reconciles exceptions.

# A Controlled Path to Go-Live

Each release should make scope, authority, evidence, and rollback posture visible before client operation begins.



| Stage             | Decision                                                                                                  | Minimum evidence                                          |
|-------------------|-----------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|
| <b>1 Scope</b>    | Is the proposed capability inside the approved solution boundary?                                         | Release manifest, products/editions, dependencies, owners |
| <b>2 Ready</b>    | Does the client environment meet access, subscription, connection, data, and security prerequisites?      | Readiness record and approved design                      |
| <b>3 Build</b>    | Are configuration changes attributable and tied to approved requirements?                                 | Configuration register and version evidence               |
| <b>4 Test</b>     | Do expected, blocked, permission, duplicate, replay, partial-failure, analytics, and recovery paths work? | Test results, defects, reconciliations                    |
| <b>5 Accept</b>   | Have authorized business roles validated the operating process and evidence?                              | UAT decision and acceptance criteria                      |
| <b>6 Cut over</b> | Are only approved components activated with smoke tests and rollback posture?                             | Cutover and smoke-test record                             |
| <b>7 Handoff</b>  | Are support, access, ownership, residual risk, and operating controls accepted?                           | Operational acceptance and support handoff                |

## Client release decision

### Approve

The proposed release is within scope, evidence is complete, residual risk is accepted, and operating ownership is ready.

### Approve with conditions

Bounded conditions, owners, due dates, monitoring, and rollback triggers are explicitly accepted.

### Hold

A missing prerequisite, untested path, access concern, unresolved defect, or commercial gap blocks activation.

### Reject or redesign

The proposed capability exceeds approved authority, control tolerance, platform capability, or contractual scope.

# Classify Before You Escalate

The response path distinguishes platform, configuration, integration, access, and client-process issues so the correct owner can act under approved authority.



| Step                 | Minimum action                                                                                                      |
|----------------------|---------------------------------------------------------------------------------------------------------------------|
| <b>1 Detect</b>      | Record reporter, time, affected process, symptoms, and evidence without spreading sensitive content.                |
| <b>2 Contain</b>     | Use authorized actions only; preserve records; avoid untested changes that expand impact.                           |
| <b>3 Classify</b>    | Separate Zoho platform issue, Acnos configuration issue, integration issue, access issue, and client process issue. |
| <b>4 Escalate</b>    | Notify the correct platform, client, and InsightVector owners under the executed agreement.                         |
| <b>5 Recover</b>     | Restore approved operation, reconcile affected transactions, and verify no duplicate or partial result remains.     |
| <b>6 Communicate</b> | Use the designated authority and agreed cadence; do not speculate about cause or scope.                             |
| <b>7 Learn</b>       | Document root cause, corrective action, owner, due date, validation, and control update.                            |

## Before go-live, document

### Declaration authority

Who can declare an incident and assign severity?

### Platform escalation

Who contacts Zoho and supplies product-specific evidence?

### Evidence preservation

Which records, logs, versions, transactions, and decisions must be retained?

### Communications authority

Who approves client, executive, contractual, privacy, or regulatory communications?

# Licensing, Support, and End-of-Service Terms

Executed documents should distinguish platform obligations, client operating responsibilities, and InsightVector service commitments.

| Topic                        | Boundary to document                                                                                                      |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------|
| <b>Zoho subscriptions</b>    | Client obtains and maintains required products, editions, capacity, and user licenses unless expressly included.          |
| <b>Feature availability</b>  | Product, edition, region, API, and portal constraints are validated during assessment and solution design.                |
| <b>Platform availability</b> | Zoho operates its services under applicable Zoho terms. InsightVector does not guarantee third-party uptime.              |
| <b>Acnos support</b>         | Channels, hours, severity, acknowledgement, escalation, maintenance, and included effort must be stated in the agreement. |
| <b>Client administration</b> | Client owns user lifecycle, policy decisions, data classification, and business continuity unless contracted otherwise.   |
| <b>Security event</b>        | Reporting path, evidence preservation, platform escalation, and communications authority are defined before go-live.      |
| <b>Data request</b>          | Export, retention, legal hold, deletion, and transition responsibilities are product- and contract-specific.              |
| <b>End of service</b>        | Revoke InsightVector access, return or delete agreed materials, preserve client records, and document open obligations.   |

## Questions procurement and legal should settle

### Who buys and maintains platform capacity?

Tie every proposed capability to the approved products, editions, users, portals, API limits, and capacity.

### What does support actually cover?

Define channels, response expectations, maintenance boundaries, third-party escalation, and excluded effort.

### How does the relationship end?

Set access revocation, export, retention, deletion, transition evidence, and unresolved-obligation responsibilities.

### Which document controls?

The executed agreement, security and privacy terms, support schedule, and applicable Zoho terms take precedence.

# A Question Set for the Proposed Release

Use the worksheet to structure the security, procurement, privacy, legal, and operating review around the exact client scope.



| Area                 | Question                                                                                                 |
|----------------------|----------------------------------------------------------------------------------------------------------|
| <b>Scope</b>         | Which Acnos capabilities, Zoho products, editions, portals, users, and integrations are proposed?        |
| <b>Architecture</b>  | Which client organization and data center will host the solution? What systems connect to it?            |
| <b>Data</b>          | What classifications, personal data, contractual records, and regulated information are in scope?        |
| <b>Access</b>        | Who approves roles, admin access, service accounts, MFA/SSO policy, and access reviews?                  |
| <b>Encryption</b>    | What product-specific controls apply in transit and at rest? Are client-managed keys required?           |
| <b>Assurance</b>     | Which certificates, SOC reports, privacy terms, and evidence apply to selected Zoho services and entity? |
| <b>DPA / privacy</b> | Which party is controller or processor for each data flow? Are DPA, SCC, or regional terms required?     |
| <b>Retention</b>     | How will records be exported, retained, placed on hold, deleted, and transitioned at termination?        |
| <b>Integration</b>   | How are connections authorized, secrets managed, API limits monitored, and failures reconciled?          |
| <b>Change</b>        | Who approves configuration releases, emergency changes, migration, and rollback?                         |
| <b>Support</b>       | What hours, severity levels, contacts, response targets, and escalation paths are contracted?            |
| <b>Incident</b>      | Who declares an incident, contacts Zoho, preserves evidence, and approves communications?                |
| <b>Continuity</b>    | What platform, client, and service recovery assumptions must be tested before go-live?                   |
| <b>Exit</b>          | How will access be revoked and client data, configuration evidence, and open support items be handled?   |

# Documents to Request Before Approval

The release package should allow a reviewer to trace scope, platform assumptions, access, data flows, test evidence, support, and acceptance without reconstructing the story.

|                                                                                                                                                                  |                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Scope and platform</b><br><br>Acnos solution scope, release manifest, products, editions, license schedule, client organization, and actual data center.      | <b>Identity and access</b><br><br>Role design, admin-access plan, service accounts, MFA/SSO position, and access-review ownership.                                               |
| <b>Data and integrations</b><br><br>Data-flow description, classifications, connection inventory, approved secret handling, API assumptions, and retention path. | <b>Configuration and migration</b><br><br>Versioned configuration register, approved change evidence, migration batches, and reconciliation results.                             |
| <b>Testing and acceptance</b><br><br>Permission, duplicate, replay, partial-failure, recovery, analytics, UAT, smoke-test, and defect evidence.                  | <b>Commercial and operations</b><br><br>Executed agreement, support schedule, privacy/security terms, incident contacts, continuity assumptions, and end-of-service obligations. |

## Release readiness cover sheet

| Field                    | Client entry                            | Field               | Client entry |
|--------------------------|-----------------------------------------|---------------------|--------------|
| Proposed release         |                                         | Decision date       |              |
| Zoho products / editions |                                         | Client data center  |              |
| Client security owner    |                                         | InsightVector owner |              |
| Open conditions          |                                         | Residual risk owner |              |
| Decision                 | Approve / Conditional / Hold / Redesign | Next review         |              |

**REVIEW  
OUTCOME**

Record the decision, conditions, owners, evidence still required, and any question that must be confirmed directly with Zoho.

# Platform Sources for Client Verification

Review the current version and product-specific scope during diligence. These references support the Zoho platform positions; they do not certify an Acnos configuration.

| Reference                | Official URL                                                                                                                                                                                                      |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Security at Zoho         | <a href="https://www.zoho.com/trust.html">https://www.zoho.com/trust.html</a>                                                                                                                                     |
| Encryption at Zoho       | <a href="https://www.zoho.com/encryption.html">https://www.zoho.com/encryption.html</a>                                                                                                                           |
| Compliance at Zoho       | <a href="https://www.zoho.com/compliance.html">https://www.zoho.com/compliance.html</a>                                                                                                                           |
| Know Your Datacenter     | <a href="https://www.zoho.com/know-your-datacenter.html">https://www.zoho.com/know-your-datacenter.html</a>                                                                                                       |
| Zoho Accounts MFA        | <a href="https://help.zoho.com/portal/en/kb/accounts/multi-factor-authentication/articles/mfa-introduction">https://help.zoho.com/portal/en/kb/accounts/multi-factor-authentication/articles/mfa-introduction</a> |
| Privacy Policy           | <a href="https://www.zoho.com/privacy.html">https://www.zoho.com/privacy.html</a>                                                                                                                                 |
| Privacy FAQ              | <a href="https://www.zoho.com/privacy/privacy-faq.html">https://www.zoho.com/privacy/privacy-faq.html</a>                                                                                                         |
| GDPR and DPA information | <a href="https://www.zoho.com/gdpr.html">https://www.zoho.com/gdpr.html</a>                                                                                                                                       |
| Zoho CRM Terms of Use    | <a href="https://www.zoho.com/crm/terms.html">https://www.zoho.com/crm/terms.html</a>                                                                                                                             |
| Zoho Terms of Service    | <a href="https://www.zoho.com/terms.html">https://www.zoho.com/terms.html</a>                                                                                                                                     |

**VERIFICATION  
RULE**

Confirm current platform documentation, legal entity, certificate validity and scope, selected product behavior, client data center, and the exact configuration before making a control or compliance decision.

This brief cites public platform material reviewed on August 21, 2026. Platform documentation and product behavior can change.

# Make Security Review Part of Release Design

A useful security review produces a bounded release decision, not a generic questionnaire detached from products, users, data, connections, and operating responsibility.



|                                                                                                                                                                                                                                                                       |                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Scope confirmation</b><br><br>Identify exact Acnos capabilities, Zoho products and editions, client organization, region, users, portals, data, and integrations.                                                                                                  | <b>Control mapping</b><br><br>Assign responsibility across Zoho, the client environment, and the contracted InsightVector delivery scope.    |
| <b>Evidence review</b><br><br>Inspect access design, data flows, release controls, test and reconciliation evidence, support, and incident readiness.                                                                                                                 | <b>Release decision</b><br><br>Approve, approve with conditions, hold, or redesign with explicit owners, evidence, dates, and residual risk. |
| <b>RECOMMENDED NEXT STEP</b><br><br>Request an Acnos security review for the proposed client scope. InsightVector will respond to questions about its contracted configuration and service controls and identify platform questions that must be confirmed with Zoho. |                                                                                                                                              |

**Acnos by InsightVector is implemented on the Zoho platform. Client Zoho licensing is separate unless expressly included.**

**[insightvectorconsulting.com](https://insightvectorconsulting.com)**

Zoho and Zoho product names are trademarks of Zoho Corporation and/or its affiliates. This brief does not replace the executed agreement, data-processing terms, security addendum, applicable Zoho terms, or the client's own vendor-risk review.