savana

Acta Technical Guide

Architecture, Governance, and Security

© 2026 Savana Inc. – All Rights Reserved.

READER GUIDE

One guide for every evaluator

Acta carries out banking work inside the conversation, through defined tools, bank policies, human confirmation, and reviewable evidence. This guide explains how the work moves through those controls and how the bank can shape the experience and intervene when needed.

01 Inside an Acta request

CTO · ENTERPRISE ARCHITECTURE

Answers: How does Acta connect to banking systems and control execution?

02 Audit and evidence

COMPLIANCE · INTERNAL AUDIT · OPERATIONAL RISK

Answers: What evidence supports review of an interaction or incident?

03 Control, containment, and recovery

CISO · SECURITY OPERATIONS · TECHNOLOGY RISK

Answers: How can the bank constrain, stop, review, and restore the work?

04 Bank-defined policies

COMPLIANCE · BANKING OPERATIONS

Answers: How does Acta apply the bank's operating policies and govern changes?

05 Bank-defined cross-selling

RETAIL BANKING · PRODUCT · CUSTOMER GROWTH

Answers: How can the bank shape relevant relationship opportunities?

ADOPT AND OPERATE

CTO, compliance, and CISO readers assess how Acta can be adopted and operated.

GROW RELATIONSHIPS

Banking and growth leaders assess its contribution to customer relationships.

Bank policy connects those perspectives by turning operating decisions into governed behavior.

01 FOR CTO ENTERPRISE ARCHITECTURE

Inside an Acta request

A banker should be able to ask a straightforward question and get to useful work. The bank should be able to explain who had access, which policies applied, and how the work was carried out.

We built Acta around that separation.

THE MODEL	THE RUNTIME	THE BANKING SYSTEM
Interprets the request and proposes the work.	Checks access, applies policy, and controls execution through defined banking tools.	Processes the operation.

Here is what that looks like for one request.

START WITH A STRAIGHTFORWARD QUESTION

Show me the recent transactions on this customer's checking account.

In this example, the banker is authenticated, has selected a customer, and has completed the verification required to view that customer's information.

1

Establish the context

Acta works from the authenticated session and its current customer context. The person's identity, the channel they are using, and their permitted capabilities establish the boundaries for the request.

The session establishes identity and access. Where additional customer context or verification is required, Acta resolves it before showing protected information.

2

Select the work

Acta identifies the capability that can carry out the request. Some work follows a specialized workflow; other requests can be handled through a defined set of tools.

A tool is a defined operation with structured inputs and an expected result. For this example, the relevant operation retrieves transaction information. The model proposes the tool call; the runtime checks its authority to proceed.

3

Check the proposed call

The request passes through server-side controls before the tool executes. Those controls check whether the capability is available in the channel, enabled for the bank, permitted for the user, and allowed under the applicable product and bank-defined policies.

Different actions need different controls. Retrieving transactions and changing an address do not have the same requirements. Verification and confirmation are applied where the operation requires them.

> **These checks run in application code, independently of the model's interpretation of the request. The bank's policies participate in the execution decision itself.**

4

Retrieve the information

If the checks permit the call, the tool requests information from the connected banking service using the session's banking identity. The banking service supplies the transaction data, which Acta uses to present the answer.

The returned information passes through the applicable response and safety controls before Acta presents it. This keeps the path from banking data to the conversational answer inside the governed runtime.

5

Present the result and retain evidence

Acta returns the information through the conversation, with structured presentation where supported. The runtime also produces governance and, where applicable, data-access evidence that can support later review.

WHEN THE REQUEST CHANGES SOMETHING

Update this customer's mailing address.

An action like this introduces a separate approval step. Once the required details are collected, Acta prepares a structured preview so the person can review the proposed action and its details. That preview does not execute the change.

The person's later confirmation is tied to the specific action and arguments held by the server. It is single-use and bound to the relevant identity and customer context. Changing the proposed details requires a new valid preview and approval; an old approval cannot simply be applied to a different action.

At confirmation, the runtime checks the approval and the applicable execution controls. The connected banking service then processes the authorized request and returns its result.

The request and approval are separate interactions:

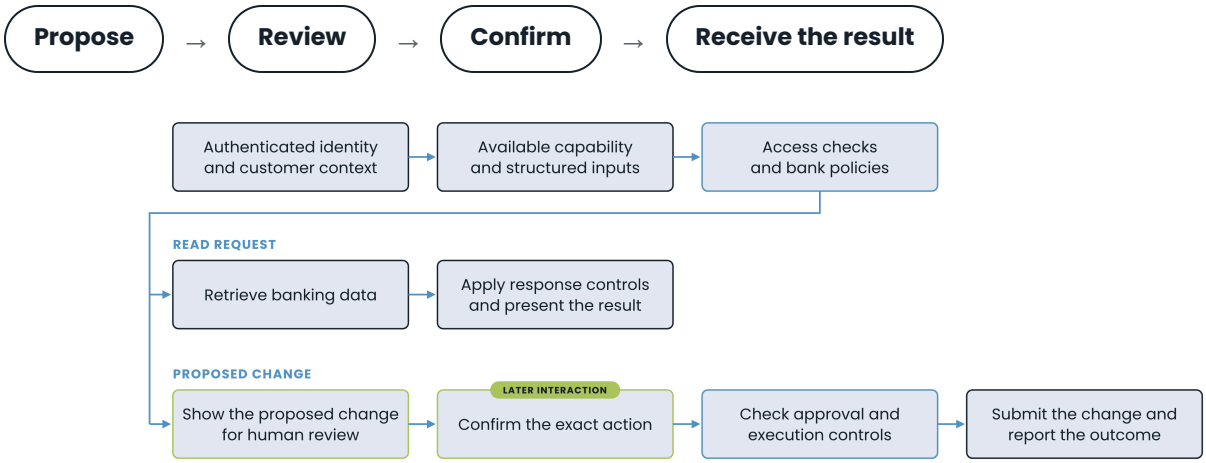


Figure 1 A request and its control path. A read request and a proposed change share the control layer. The change adds a separate human approval step.

What this gives the bank

The conversational interface can make servicing easier while keeping authority explicit.

Identity comes from authentication.

Access comes from permissions.

Policy is evaluated by the runtime.

Approval is tied to a specific change.

Results come from the systems performing the work.

That separation lets the experience remain conversational while the work follows the bank's controls.

02 FOR COMPLIANCE INTERNAL AUDIT OPERATIONAL RISK

Audit and evidence

When a compliance or security team reviews an Acta interaction, it needs evidence it can inspect: the policy decision, the recorded control events, and the integrity of the retained history.

We built Acta to produce structured evidence as the runtime makes those decisions. A reviewer can examine the recorded facts directly, alongside the conversation and the banking-system result.

Evidence with a defined purpose

Governance decisions

HASH-CHAINED

Review of policy evaluation results, recorded reasons and requirements, and authorization decisions.

Administration and security events

HASH-CHAINED

Review of configuration changes, security interventions, emergency controls, and recorded execution failures.

Data-access records

Review of recorded customer-data access by principal and tool.

AI operational telemetry

Monitoring of model behavior, performance, and usage over time.

Acta's governance and administration/security audit streams are **hash-chained**, with a separate chain for each bank and stream. Data-access records and operational telemetry provide complementary evidence for investigation and oversight.

How the hash chain works

A cryptographic hash is a fingerprint calculated from data. Acta uses SHA-256 to calculate each audit entry's fingerprint from its covered record fields and the preceding entry's hash.

The next entry incorporates that fingerprint into its own calculation. Repeating this process connects the records in order.

This entry's hash = hash of this entry's covered data and the previous entry's hash.

Verification recalculates the hashes and checks the links in the retained sequence. Changing a covered value without updating its hash creates a mismatch. Removing a record from the middle breaks the expected link to the next retained record.

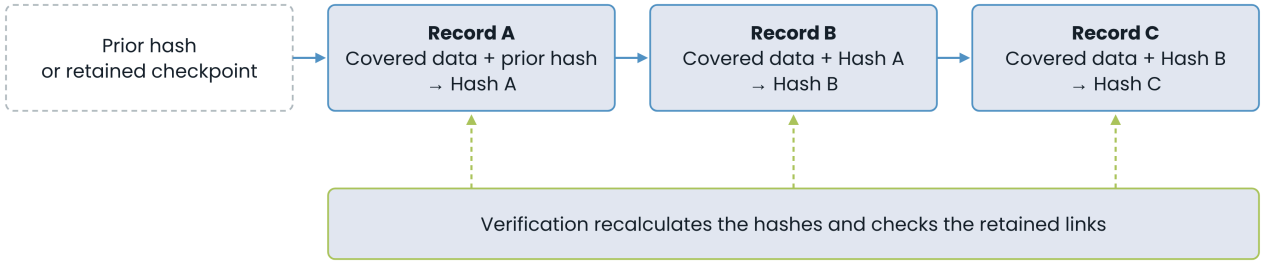


Figure 2 Hashes connect the retained audit records.

The result is a tamper-evident audit trail with a repeatable integrity check.

The bank can test the retained evidence using the recorded data and the chain itself.

Follow the decision and the outcome

Acta records a governance decision at authorization time, before the tool executes. That preserves what the policy engine decided at the point the decision mattered.

Execution and banking-system evidence then establish the outcome of the operation. Keeping these facts distinct gives reviewers a clear structure for investigating a request:

1. **What was proposed**
2. **What was permitted**
3. **What result was returned**

The same approach applies to operational control. Emergency-stop activation, reviewed restoration, and quarantine clearance produce administrative evidence. Security teams can review the intervention as well as the activity that prompted it.

Retain continuity as records age

Acta's retention mechanism preserves the continuity of the remaining chain. When eligible older records are removed from the beginning of the sequence, a checkpoint is retained at that boundary. Subsequent verification starts from that checkpoint.

This lets the bank apply its retention policy while maintaining an integrity check over the history it retains.

Bring the evidence into the bank's security operations

Acta supports authenticated retrieval and signed delivery of selected audit records to the bank's security information and event management system, or SIEM. The integration brings Acta's evidence into the bank's established monitoring and investigation processes.

Practical ways to examine the system's activity

Hash-chain verification

Recalculates the hashes and checks the links in the retained sequence.

Controlled retention

A checkpoint is retained at the boundary. Subsequent verification starts from that checkpoint.

Security export

Authenticated retrieval and signed delivery of selected audit records to the bank's SIEM.

Hash-chain verification, controlled retention, and security export give compliance and security teams practical ways to examine the system's activity. The evidence is structured for review from the start.

03 FOR CISO SECURITY OPERATIONS TECHNOLOGY RISK

Control, containment, and recovery

A CISO needs to know how an AI system is constrained, how the bank can intervene, and who decides when it can resume work. We built those controls into Acta's runtime and administration model.

The bank can limit available capabilities, stop tool execution across its Acta environment, and review sessions that have been quarantined by safety monitoring. Recovery follows defined permissions and review paths, with evidence of the changes made.

Control access before execution

> **Acta separates the model's interpretation of a request from the authority to carry it out.**

Tool availability, authenticated identity, role permissions, and policy evaluation determine whether a proposed call can proceed.

Banker and customer channels expose their own permitted capabilities. Specialized workflows operate within the user's permissions. The same control model applies as the conversation moves from a question to a proposed banking action.

Input and output safety controls, structural validation, and checks on the origin of action parameters support this boundary. These controls run alongside authorization and confirmation in the execution path.

Emergency Stop

Emergency Stop gives an authorized bank operator a direct containment control over Acta tool execution.

Once active in the runtime, the stop blocks new tool invocations for that bank. The bank can see which runtime instances have acknowledged the change, giving operations a way to verify that containment has taken effect.

A fast path to containment

Activation is an immediate administrative command, with a recorded reason and audit evidence. It does not wait for the normal configuration approval queue.

A controlled path back to service

Restoring service follows a different path: deactivation requires a reviewed proposal and an approver distinct from the person who submitted it.

Quarantine an affected session

Acta's session monitoring evaluates safety signals such as repeated blocked content, rejected actions, and failures of action-parameter checks. When configured thresholds are crossed, the affected session can be quarantined automatically.

Quarantine blocks guarded actions such as transfers, wires, and controlled case or work-item changes in that session. This gives the bank a focused response while it reviews the activity.

An authorized reviewer can inspect the quarantined session and clear it with a recorded reason. Clearance is tied to that session's current control state. Review deadlines and escalation behavior are governed settings; configured escalation can terminate an overdue session and stop further tool use from it.

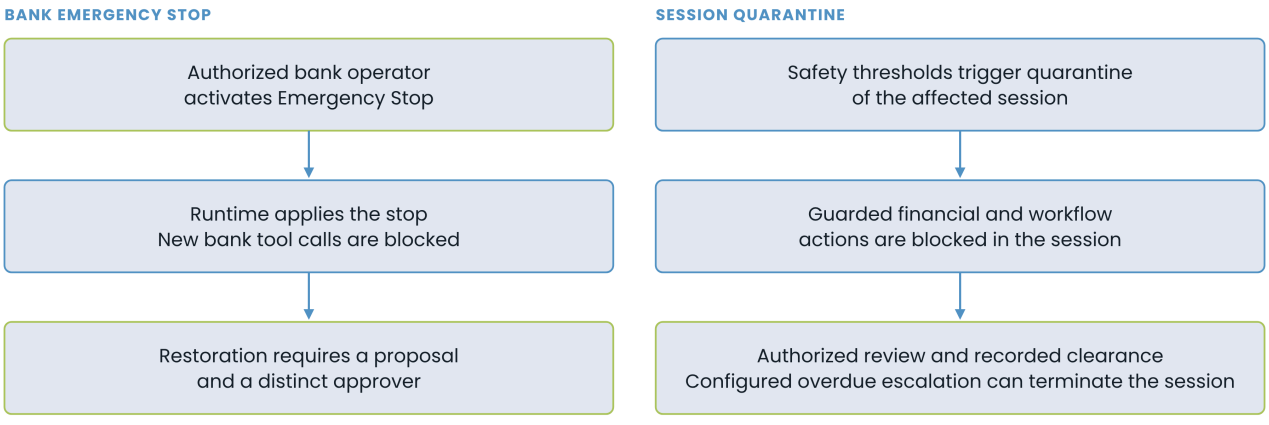


Figure 3 Bank and session containment with controlled recovery.

Choose the appropriate level of intervention

These controls give security and operations teams choices at the capability, session, and bank levels.

CAPABILITY LEVEL

Tool or workflow availability

BANK OBJECTIVE

Decide which capabilities the bank makes available.

PATH BACK TO SERVICE

Reviewed configuration change and runtime adoption.

SESSION LEVEL

Session quarantine

BANK OBJECTIVE

Contain guarded actions in a session that has crossed safety thresholds.

PATH BACK TO SERVICE

Authorized session review and recorded clearance.

BANK LEVEL

Bank Emergency Stop

BANK OBJECTIVE

Block new Acta tool invocations across the bank's environment.

PATH BACK TO SERVICE

Reviewed deactivation with a distinct approver.

Verify the control is in effect

Administrative intent and runtime adoption are visible separately. For changes such as an emergency stop or a policy update, Acta records the change and tracks acknowledgement by the relevant runtime instances.

That gives the bank an operational answer to "Has the control taken effect?" It also provides evidence for the review that follows: who intervened, why, which change was applied, and how recovery was authorized.

The ability to intervene is part of the product. So is the ability to verify the intervention and govern its reversal.

04 FOR COMPLIANCE BANKING OPERATIONS

Bank-defined policies

The bank defines how it operates. Acta applies those policies when work is requested, with a clear record of the resulting decision.

Acta gives the bank a way to put its operating rules into the execution path. Bank-defined policies shape which actions can proceed, when a warning is needed, and which approved guidance should accompany the work.

Define the operation and the circumstances

A bank can define policies for particular operations and circumstances, choose the channels where they apply, and specify the response when their conditions are met.

The policy engine evaluates those conditions against the proposed tool call and the relevant session, customer, and account context. Bank-authored policies can:

- **Stop an operation**
- **Raise a warning**
- **Supply approved guidance**

A blocking policy is enforced before the tool body executes.

Apply the policy at the point of action

FOR EXAMPLE, A BANK COULD

Prevent an account from being closed while pending transactions remain.

Evaluate
When the operation is requested, Acta evaluates the relevant account state against that policy.

→

Stop and explain
If the condition matches, the operation is stopped and the restriction can be explained in the conversation.

→

Record
The governance evidence records the authorization decision and the triggered policy reference.

This connects the bank's written operating intent to a control applied during the work.

Bring approved guidance into the conversation

The bank can also maintain its approved procedures and disclosures as governed content. That brings the bank's operating guidance into the work at the point where it is relevant.

The bank controls the guidance, and the policy context determines where it is used. Bankers and customers receive language that reflects how the institution wants the interaction handled.

Review changes and verify adoption

Policy changes and bank content follow a reviewed administrative process. An authorized person proposes the change and records a reason. Another authorized person reviews it before application.

Propose with a reason → **Review by another person** → **Apply** → **Track adoption**

The platform retains the proposal, review, and application evidence, including the revision the change was based on. Approved runtime changes are tracked through adoption so the bank can see whether the intended configuration has taken effect.

One process, three perspectives

For a CTO
A way to adapt behavior through governed configuration.

For compliance
It makes the bank's rules and approved language reviewable.

For a CISO
It keeps changes to AI behavior inside an authorized, traceable process.

05 FOR RETAIL BANKING PRODUCT CUSTOMER GROWTH

Bank-defined cross-selling

The bank knows the relationships it wants to grow and the conversations it wants to encourage. Acta gives it control over when a cross-sell opportunity appears, how it is prioritized, and how it is introduced.

Opportunity rules turn available customer and account information into relevant observations that a banker or customer can choose to explore.

Define what is worth bringing up

Acta provides an opportunity-rule library that the bank can tailor to its own relationship strategy. The bank can configure:

The conditions
Which available customer, account, or relationship facts should trigger an opportunity.

The audience
Whether the opportunity appears in the banker or customer channel.

The priority
How the matched observation is classified and prioritized.

The presentation
The wording and suggested next step shown to the banker or customer.

The availability
Which opportunity rules are enabled for the bank.

Those settings let the bank shape the experience from the conditions that surface an opportunity to the language that introduces it.

From a relationship fact to a useful conversation

CONSIDER

A customer with a checking account and no savings relationship.

A bank-defined opportunity rule can identify that combination and surface a prompt to discuss savings. The path is straightforward:

1. Acta evaluates available relationship information against the bank's effective rule.
2. A match produces a structured observation with its configured priority and wording.
3. The banker or customer can choose the suggested next step.
4. Any subsequent banking operation follows its access, policy, and confirmation controls.

The opportunity has an identifiable starting point: a defined rule matched a set of facts.

The model can then help explain the observation and continue the conversation.

Keep the bank in charge of the experience

Changes to opportunity rules follow a reviewed administrative process. An authorized person proposes the override and records a reason. Another authorized person reviews it before application, with proposal, review, and application evidence retained.

This gives the bank a practical way to refine its cross-selling approach as priorities change.

It controls the criteria, the prominence, and the message, while Acta brings the relevant opportunity into everyday servicing.



© 2026 Savana Inc. – All Rights Reserved.