PINNACLE

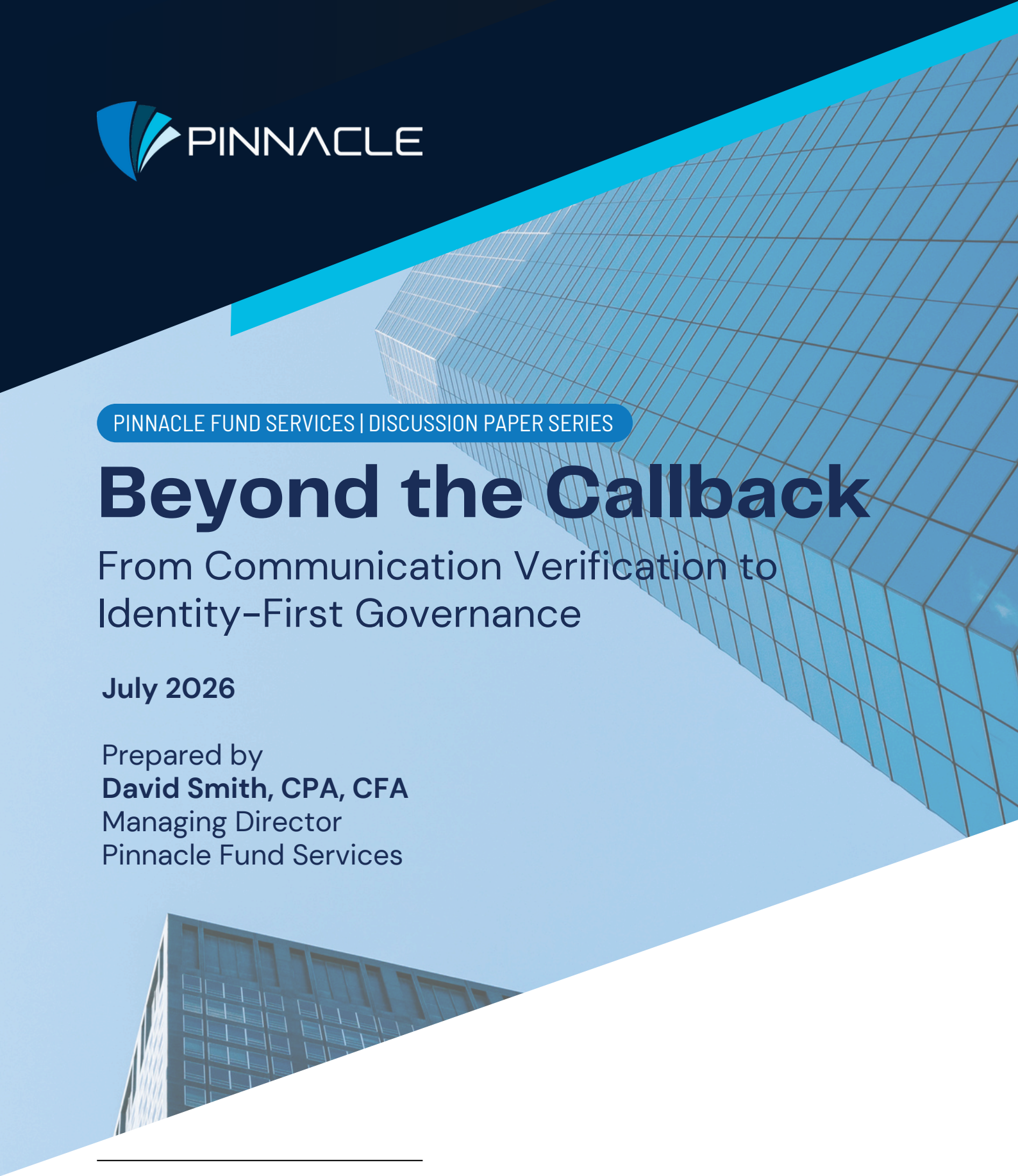
PINNACLE FUND SERVICES | DISCUSSION PAPER SERIES

Beyond the Callback

From Communication Verification to Identity-First Governance

July 2026

Prepared by
David Smith, CPA, CFA
Managing Director
Pinnacle Fund Services



Investor change management has evolved beyond traditional callback procedures. This discussion paper proposes a governance framework built on identity, authority, governance, shared awareness, and integrity to strengthen investor protection and operational resilience across private fund administration.

EXECUTIVE SUMMARY

For more than twenty years, the callback has functioned as one of the load-bearing controls of private fund administration. It arose because administrators had no dependable way to know whether an emailed, telephoned, faxed, or mailed instruction genuinely came from the investor who appeared to send it. Calling the investor back on a previously known number closed that gap.

Over time the practice hardened into an industry norm. Auditors, regulators, and fund managers alike came to treat a completed callback as proof that an investor change had been properly controlled.

The environment that made the callback indispensable has fundamentally changed. Investors now reach administrators through authenticated portals, multi-factor login, role-based permissions, and workflow platforms that log every step of a transaction. Investor structures have grown more layered, cyber threats more capable, and regulatory expectations more exacting, while investors themselves expect the same authenticated experience they already receive from their banks.

That shift matters because it relocates the point at which an organization can first place confidence in a request:

- **Under the callback model,** trust had to be manufactured after a request arrived, because nothing about the request itself could be trusted on receipt.
- **Under an authenticated model**, trust can exist before the request is ever submitted. Governance no longer needs to start by asking whether a message is genuine; it can start by asking what an already-known individual should be allowed to do.

This paper argues that private fund administrators should respond to that shift not by refining the callback, but by **replacing communication verification as the organizing purpose of investor change management**. In its place, the paper proposes a five-part governance model — the **Chain of Trust** — built around identity, authority, governance, shared awareness, and integrity. Each principle answers a distinct question about a proposed investor change; together they cover the full lifecycle of that change, from the moment a request is made to the moment it becomes part of the permanent investor record.

None of this diminishes what the callback accomplished. It solved the problem it was built to solve, and for much of the industry's history there was no better tool available. The argument here is narrower and more specific:

a completed callback answers only one governance question, and modern investor servicing depends on answering several more.

The question worth asking is no longer whether the callback happened. It is whether trust was established before the request entered the organization, whether the request was governed in proportion to its risk, and whether the resulting record can be relied upon long after the transaction is closed.

1. WHY THE CALLBACK BECAME STANDARD PRACTICE

Operational controls tend to survive because they solve a real problem well, not because they are elegant or efficient. The callback is a good example. It was never a sophisticated piece of technology — a phone call to a known number — yet for decades it was one of the most trusted safeguards in private fund administration, because it addressed a problem every administrator faced: sensitive instructions arrived through channels that offered no inherent assurance of authenticity.

Before the emergence of secure digital channels, investor servicing ran almost entirely on unauthenticated correspondence. Requests to change banking details, update contact information, appoint a representative, or amend distribution elections arrived by email, phone, fax, or letter, and administrators had no built-in way to confirm that the sender was who they claimed to be.

Several factors compounded that uncertainty:

- Email addresses could be spoofed.
- Signatures could be copied.
- Representatives left their roles, finance teams reorganized, and contact details went stale — even when nothing improper was intended.

Administrators were left to distinguish a legitimate instruction from an outdated or fraudulent one using only the document in front of them.

The callback addressed that risk directly. Rather than accepting the incoming message at face value, the administrator independently reached the investor through contact information established beforehand, outside the channel the request had arrived on. That independent step meaningfully reduced the odds that a fraudulent or mistaken instruction would be processed, and it gave the industry a repeatable, well-understood discipline to apply to sensitive requests. Fund managers came to associate it with prudent administration; auditors came to treat it as evidence of a controlled process.

That track record deserves to be taken seriously. **Sound governance is not built by discarding controls that work**; it is built by understanding why a control was introduced, what conditions it assumed, and whether those conditions still hold. The relevant question, then, is not whether the callback was the right answer for its time. It is whether the assumptions that made it indispensable are still true today.

Those assumptions have not aged well:

- Institutional investors are larger and structurally more complex than they were twenty years ago, frequently maintaining several authorized representatives with different levels of delegated authority.
- Operational platforms have become integrated rather than siloed.
- Cyber threats have grown more sophisticated, and regulators expect demonstrable governance over investor data as a matter of course.
- Investors now interact with banks, brokerages, and insurers through authenticated digital channels as a matter of routine, and increasingly expect the same from fund administrators.

Despite all of this, a great many investor servicing processes still begin exactly where they began two decades ago — with an unauthenticated communication that must be verified before anything else can happen. That was a reasonable starting point when no better option existed. It is a much less obvious starting point now that better options exist. The remainder of this paper explores what changes when trust no longer has to be manufactured after the fact.

2. WHAT CHANGED, AND WHY IT MATTERS

The technological shift described above is easy to summarize, but its implication is easy to understate: it does not simply give administrators a faster or more convenient way to do what the callback already did.

It changes which questions investor change management is supposed to answer in the first place.

Under the old model, once a communication had been verified, everything downstream — updating records, notifying interested parties, retaining documentation — tended to be treated as separate administrative processes rather than as connected parts of one governance process. That made sense at the time, because verifying the communication was, in practical terms, the hard part; everything after it felt comparatively mechanical.

That is no longer an accurate picture of what a banking-instruction change, or any comparably sensitive investor request, actually involves. Such a change can touch:

- capital distributions;
- tax reporting;
- anti-money-laundering records;
- regulatory filings; and
- every downstream system that depends on the investor record being correct.

A request that is processed without adequate authority checks, proportionate oversight, or stakeholder visibility carries risk regardless of how convincingly the original communication was authenticated. The scope of what needs governing has grown well beyond the scope of what a callback was ever designed to check.

3. FROM COMMUNICATION-FIRST TO IDENTITY-FIRST GOVERNANCE

It is worth stating plainly what has changed and what has not. **Authentication technology does not remove the need for governance** — if anything, it raises the bar for what governance is expected to accomplish. What it removes is the need to spend scarce administrative attention on a question — is this communication genuine? — that can now be answered before the request is even submitted.

Framed as a single question, the old model asked: can this communication be trusted? An identity-first model asks a broader set of questions instead:

- Who is interacting with the organization, and has that identity already been established?
- Is this person authorized to take the action requested?
- Does the request's sensitivity call for additional review?
- Which stakeholders need to remain aware of it as it moves through the process?
- Can every step be reconstructed later through a complete record?
- Can the resulting investor information be relied upon?

A callback, executed flawlessly, answers only the first of those questions. It says nothing about whether the person confirming the change still holds the authority to do so, whether anyone else who should know does know, whether the level of review matched the risk involved, or whether every system touched by the change now agrees with every other system. None of that is a criticism of the callback — it was never built to answer those questions. It is, instead, the reason a broader framework is needed.

This is the essential shift from a **communication-first** to an **identity-first** model:

- In the *communication-first model*, trust enters the process after a request arrives and has to be earned through verification before governance can proceed.
- In the *identity-first model*, trust already exists at the point of interaction, because identity has been authenticated in advance; governance can begin immediately and concentrate on the judgment-intensive questions of authority, proportionate oversight, transparency, and record integrity.

The shift does not make governance less important. **It makes governance the whole point**, rather than an afterthought to communication verification.

4. THE CHAIN OF TRUST: A FIVE-PRINCIPLE FRAMEWORK

If trust can be established before a sensitive request is accepted, investor change management needs a structure built around that fact — not a longer checklist bolted onto the existing process, but a framework in which each stage reinforces the one that follows.

This paper refers to that structure as the **Chain of Trust.**

Unlike a model built around one dominant control, the Chain of Trust treats confidence as something accumulated progressively across the life of an investor change, through five connected principles, each answering a distinct governance question:

Principle	Governance Question It Answers
Identity	Who is interacting with the organization?
Authority	Is this person permitted to take this action?
Governance	Does this request need additional oversight?
Shared Awareness	Who else should know this is happening?
Integrity	Can the resulting record be trusted?

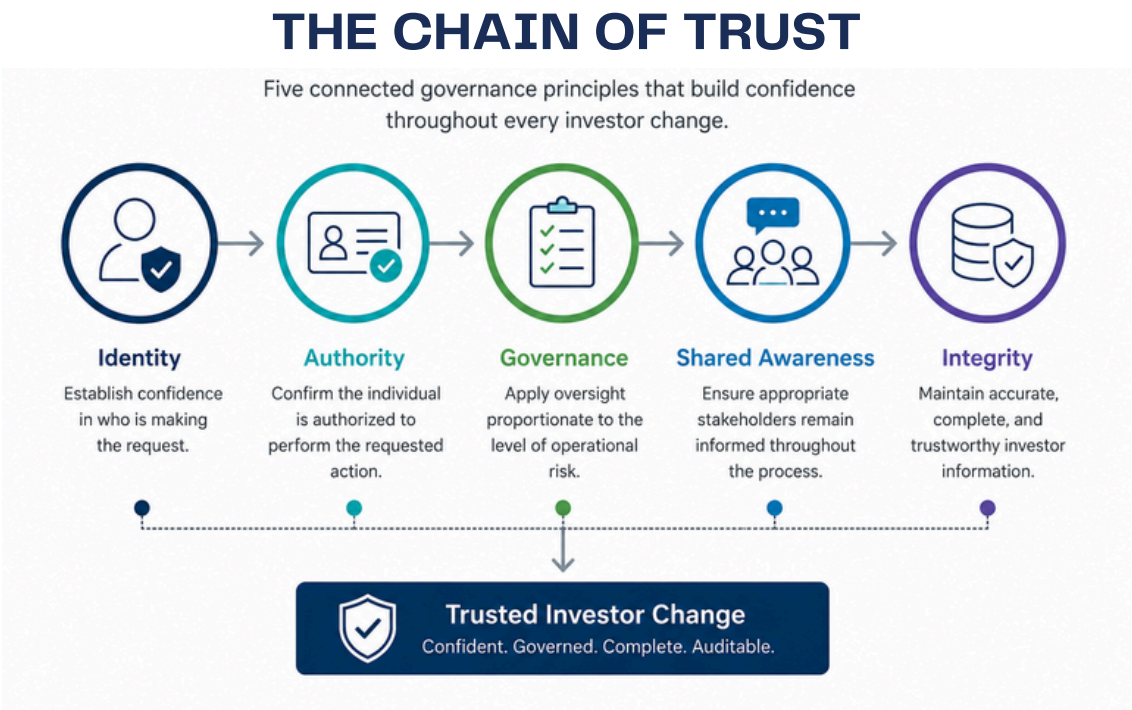


Figure 1. The Chain of Trust — five connected governance principles that build confidence throughout every investor change.

No single principle is sufficient on its own. Knowing who someone is does not establish what they may do. Knowing what they may do does not establish how much scrutiny a given request deserves. Rigorous approvals accomplish little if the resulting information is then recorded inconsistently across an organization's systems.

The value of the framework lies in the sequence:

- **Identity** gives confidence in the individual.
- **Authority** gives confidence in their permissions.
- **Governance** calibrates oversight to risk.
- **Shared Awareness** keeps the right people informed as the change moves forward.
- **Integrity** ensures every decision made along the way survives intact in the permanent investor record.

Taken together, these principles reorient investor servicing away from verifying incoming messages and toward governing investor information throughout its lifecycle. Each is examined in turn below.

4.1 Identity: The Starting Point

Every governance process depends on a first, reliable answer to a simple question: **who is interacting with the organization?** Without that answer, nothing that follows can be evaluated with real confidence — not authority, not the appropriate level of scrutiny, not whether the request should proceed at all.

Under the older model, this question could only be approached retrospectively, by examining what had arrived: comparing an email address or signature against what was on file, checking supporting documents, or calling the investor back. Identity, in effect, had to be inferred from the communication itself.

Authenticated access changes the order of operations. Multi-factor login, controlled access, and modern identity management let an organization know who it is dealing with before a sensitive request is ever submitted, rather than trying to reconstruct that fact afterward.

This is a meaningful change in what administrators spend their time doing. Once identity is no longer in question, the expertise that used to go into establishing it can go instead into judgment calls that genuinely require experience:

- whether this person is authorized for this specific action;
- whether the request's risk profile warrants extra review;
- who else ought to be told; and
- how the resulting change should be reflected across the organization's records.

Identity, in short, is not a replacement for the callback bolted onto the front of the process. **It is what makes the rest of the framework possible** — the trusted starting point every subsequent governance decision depends on.

Figure 2. Identity Before Communication — establishing authenticated identity before a request is accepted strengthens every governance step that follows.

4.2 Authority: Knowing Who Someone Is Does Not Determine What They May Do

Establishing identity answers only the first governance question; it says nothing about what an authenticated individual is actually permitted to do. That distinction matters more than it once did, because investor structures have grown more layered. Institutional investors commonly maintain several authorized representatives with different delegated powers:

- a **treasury contact** may have no authority over legal ownership records;
- **counsel** may be authorized to execute documents but not to change payment instructions; and
- a **senior executive** may delegate day-to-day operational authority while retaining sign-off on the decisions that matter most.

Confusing authentication with authority creates a specific, avoidable risk: a person can log in successfully and no longer hold the authority to change banking details or appoint new users, while someone else with continuing authority may be entirely unaware a request has been made in their organization's name.

The deeper problem is that authority records are too often treated as static — collected once during onboarding and left largely untouched afterward. Organizations, however, do not stay still:

- Directors retire.
- Finance functions get reorganized.
- Advisors change.
- Mergers or restructurings redraw governance lines.

The individuals entitled to instruct an administrator on an investor's behalf shift continually over the life of an investment, and authority records need to shift with them or they gradually turn into historical artifacts rather than an accurate picture of who currently holds authority.

Treating **authority as living information** — reviewed periodically, updated as circumstances change, and built into the governance workflow rather than filed away as supporting documentation — also changes what a routine control like a pre-distribution banking confirmation is for. Confirming an account number before capital leaves the fund is sound practice as far as it goes. But that confirmation can accomplish more: it can also verify that the person responding still holds the authority to respond, trigger additional review where warranted, and refresh the organization's authority records as part of the same step.

Handled this way, a periodic confirmation stops being a narrow pre-payment check and becomes a **governance event in its own right** — one that reinforces confidence in the investor relationship as a whole, not just in a single account number.

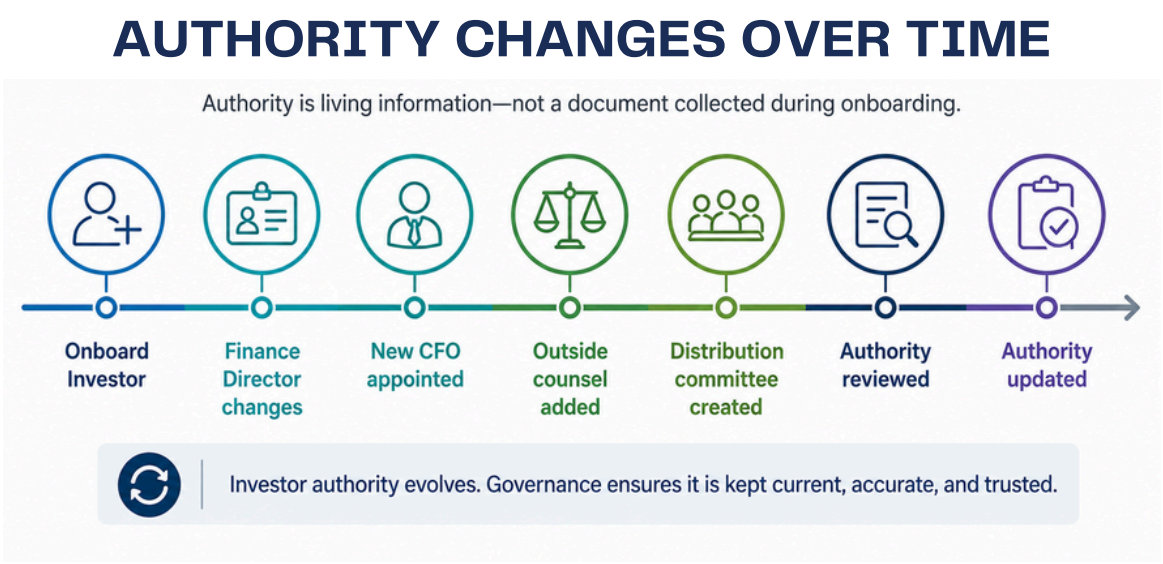


Figure 3. Authority Changes Over Time — authority is living information that must be reviewed and updated as an investor's governance structure evolves.

4.3 Governance: Matching Oversight to Risk

Once identity and authority are settled, attention shifts from the person making the request to the request itself. Not every investor change carries the same weight. Updating a mailing address and changing banking instructions are not comparable events and treating them as though they were equivalent allocates scrutiny where it adds little value while potentially under-scrutinizing the changes that matter most.

Many organizations have historically applied fairly uniform procedures across broad categories of requests, which promotes consistency but spends administrative effort without regard to the actual risk of what is being changed. A more effective approach calibrates oversight to risk:

- **Higher-risk changes** warrant segregation of duties, multiple approvals, and closer documentation.
- **Lower-risk changes** can move through lighter, faster workflows without weakening the overall control environment.

The payoff is not only efficiency, though that matters. It is that experienced staff end up spending their judgment where it is actually needed, rather than distributing it evenly across requests that differ enormously in consequence. Good governance, on this view, is not measured by how many approvals a process requires. **It is measured by whether the level of scrutiny applied to a given request actually matches the risk that request presents.**

4.4 Shared Awareness: Visibility as a Control in Its Own Right

Sound decisions are not, by themselves, sufficient. Governance also depends on the right people knowing that a decision is being made — before, during, and after it happens. Investor servicing has traditionally been a fairly private affair: a request comes in, an administrator processes it, records are updated, and whether anyone beyond the administrator and the investor becomes aware of the change is often a matter of informal habit rather than deliberate design. In many cases, a change affecting an investor's assets may be known to exactly one person inside the organization at the time it happens.

That pattern creates **operational blind spots** — conditions in which authority changes without review, records get updated without oversight, or important knowledge exists only in one person's head. The immediate danger is not necessarily that something goes wrong; it is that if something does go wrong, there is no structural reason it would be noticed until well after the fact.

Designing this risk out means making sure appropriate stakeholders know:

- when a significant request has been submitted;
- whether approvals are still pending; and
- when the change has actually been completed.

This does not mean generating more notifications — it means building visibility into the process itself rather than leaving it to chance. When that visibility exists:

- unusual activity is easier to spot;
- errors are more likely to be caught before they reach an investor; and
- unauthorized activity becomes far harder to conceal quietly.

It also makes governance less dependent on any one administrator's memory or tenure, which strengthens the resilience of the process and makes it easier to explain to auditors and regulators after the fact.

The goal is not to involve more people in every decision. It is to make sure the people who are responsible for protecting investor interests are never the last to find out about a change that affects them.

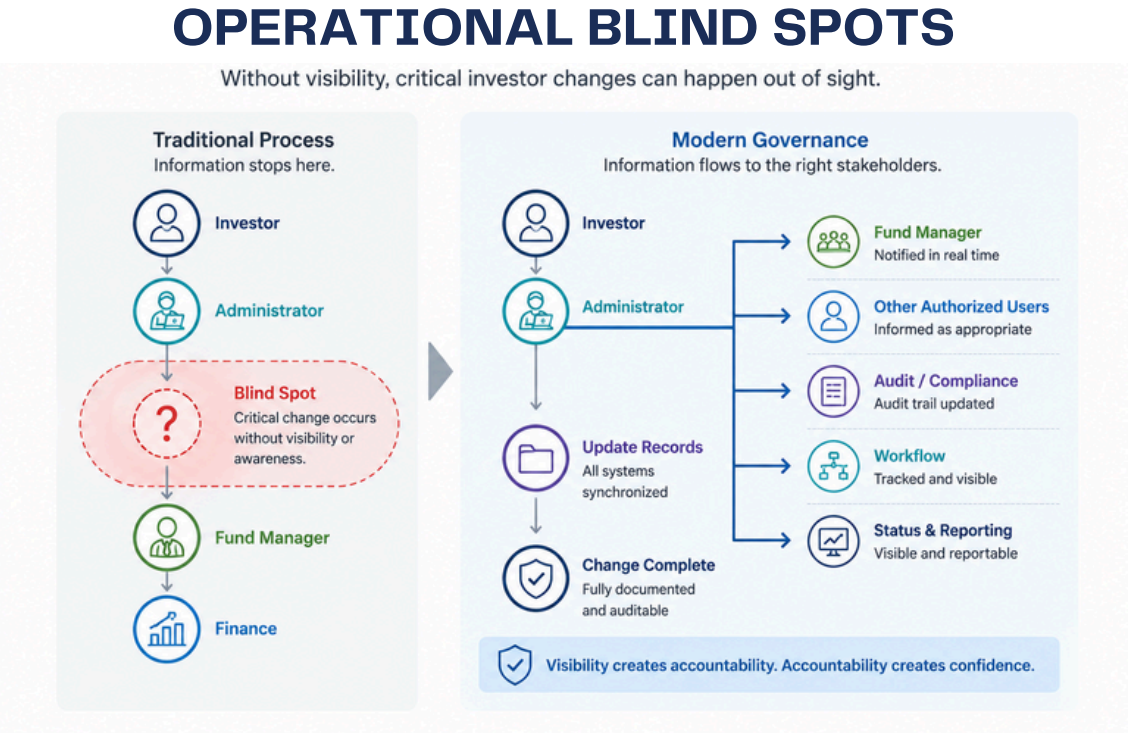


Figure 4. Operational Blind Spots — without deliberate visibility, critical investor changes can occur unnoticed; modern governance routes information to every stakeholder who needs it.

4.5 Integrity: One Record the Organization Can Trust

Every governance process eventually produces the same kind of output: information. However carefully a request was authenticated, authorized, reviewed, and approved, the process has not truly succeeded if the investor record that results is inaccurate, incomplete, or inconsistent with what other parts of the organization believe to be true.

> **Governance does not end at approval — it ends when the record reflects the decision correctly.**

This has become a harder problem as operating environments have grown more interconnected. A single banking-instruction change can touch:

- a transfer agency platform;
- a payment system;
- a CRM;
- an investor portal;
- document storage;
- workflow tools; and
- compliance and reporting databases — all at once.

Every manual re-entry of the same fact into a different system is another chance for it to diverge from the original decision.

Most operational failures in this area do not trace back to a wrong decision. They trace back to a correct decision being implemented unevenly — one system updated, another missed, payment details that no longer match across platforms, a contact record current in one place and stale in another. Left unaddressed, an organization ends up with several competing versions of the same investor fact and no reliable way to know which one is right.

The fix is structural rather than procedural: a single trusted investor record that serves as the authoritative source feeding every downstream process, so information is captured once, governed carefully, and referenced consistently rather than re-entered and re-verified in each system that needs it. This is frequently discussed as an efficiency question, but it is really a governance question — fewer duplicate entries means fewer chances for inconsistency and greater confidence that every part of the organization is working from the same governed facts.

Integrity is what makes the rest of the framework durable. Identity confirms the individual, authority confirms their permissions, governance calibrates the oversight applied, and shared awareness keeps the right people informed — but if the resulting record does not accurately capture all of that, the value of everything upstream erodes. Get integrity right, and an organization has something more valuable than a clean database: a record that can be relied upon wherever it is used, months or years after the original decision was made.

5. THE ROLE OF TECHNOLOGY

Technology's most useful contribution to this framework is not automation for its own sake. It is freeing experienced staff from repetitive administrative work so they can spend more time on the judgment calls that actually protect investors.

> **Technology should not substitute for that judgment; it should absorb the manual tasks that consume time without improving governance.**

A great deal of traditional investor servicing involves entering the same fact into several different systems:

- a transfer agency platform;
- a payment application;
- a CRM;
- a workflow tool;
- a document repository; and
- an internal reporting database.

Each individual update looks routine in isolation, while the cumulative effort and inconsistency risk add up considerably. A better-designed environment captures information once, governs it properly, and makes it available everywhere it is needed, using workflow automation to coordinate approvals and notifications to improve visibility, rather than adding administrative burden of its own.

The resulting benefit is not simply speed. It is **better governance**, because staff whose time is no longer consumed by repetitive re-entry can instead focus on evaluating authority, weighing operational risk, applying proportionate oversight, and resolving exceptions — responsibilities that remain fundamentally human even in a highly automated environment.

The right question for an organization to ask is therefore not how technology can automate investor servicing, but how it can free governance professionals to spend more of their time exercising judgment and less of it repeating tasks a system could just as easily handle.

6. REVISITING THE CALLBACK: WHAT IT DOES, AND DOES NOT, ANSWER

It is worth returning to the question this paper opened with:

What problem does a callback actually solve?

For a long time the answer was simple enough — it confirmed, independently, that an investor had actually requested a change before the organization acted on sensitive information. In an environment where requests arrived through channels that offered no built-in assurance, that was a genuinely useful safeguard.

But it was always a narrow one. A callback establishes confidence in a communication. It says nothing, by itself, about authority, about who else should have known, about whether the level of review matched the risk, or about whether every affected system now agrees.

Consider a routine example. An administrator receives a request to change banking instructions. A callback confirms the request, the investor verbally acknowledges it, and the record is updated. As a matter of communication verification, this process has gone exactly as intended.

As a matter of governance, several questions may remain open:

- Did the person who confirmed the change still hold authority to instruct on banking details?
- Should another authorized representative have been notified before payment details changed?
- Did the request's significance warrant heightened review?
- Were all the systems that reference banking information updated consistently?
- Could the organization reconstruct, from a complete record, exactly how this decision was made months later if asked to?

None of this means the callback failed — it performed exactly the function it was designed for. It means the framework surrounding it, not the callback itself, is what determines whether those remaining questions get answered. That is precisely why investor change management should not continue to be organized around communication verification as its central purpose.

> **Communication is one input to a governance process, not the whole of it.**

The more durable question is not "did we complete the callback," but:

- whether identity was established before the request entered the process;
- whether authority was confirmed;
- whether oversight matched the risk;
- whether the right stakeholders were informed; and
- whether the resulting record can be relied upon with confidence.

The callback answered the question the industry most needed answered twenty years ago. **The questions that matter now are broader.**

WHAT A CALLBACK VERIFIES – AND WHAT IT DOESN'T

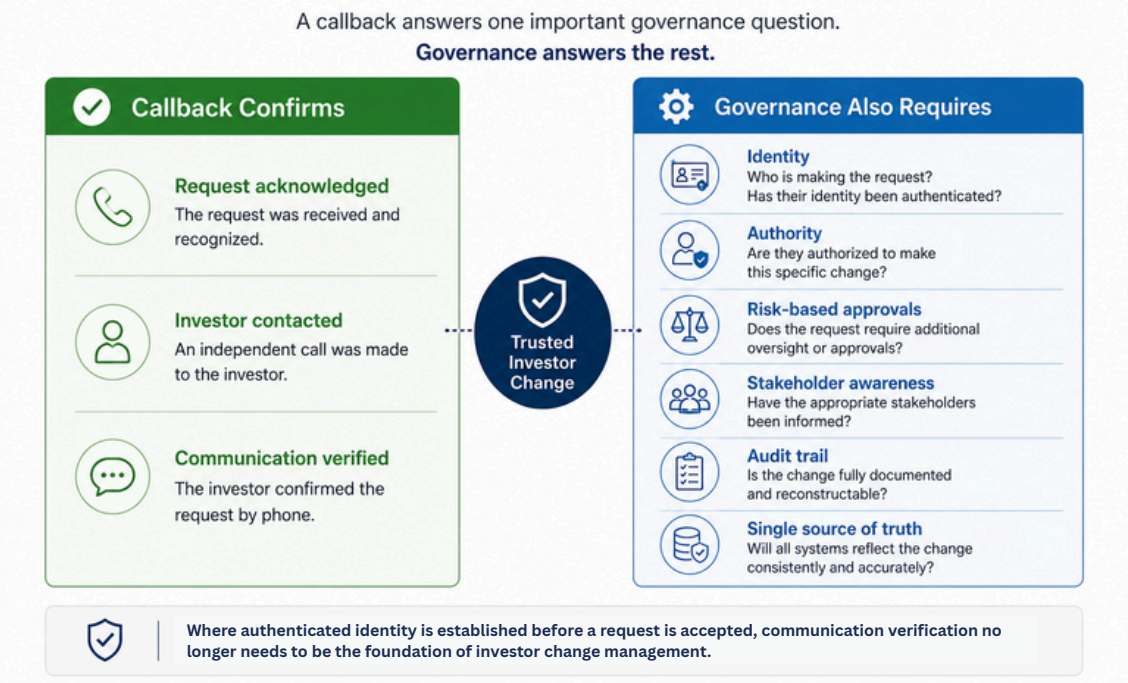


Figure 5. What a Callback Verifies — and What It Doesn't. A callback confirms that a communication is genuine; governance must still answer the questions of identity, authority, oversight, transparency, and record integrity.

7. PUTTING THE FRAMEWORK INTO PRACTICE

This paper does not prescribe a single technology platform or operating model — fund managers and administrators differ too much in regulatory environment, investor base, and existing capability for a one-size answer to be useful. The principles behind the Chain of Trust, however, are meant to generalize across those differences.

A useful starting exercise for any organization is to ask, plainly, **where trust first enters its investor change process**. If confidence is only established once an email or phone call has been received and verified, the organization is still operating a communication-first model — a reasonable model for the environment it was built in, but one that predates the authentication, workflow, and identity tools now widely available.

The opportunity is to redesign the process so that trust is established before a sensitive request is accepted, freeing governance to focus on authority, proportionate oversight, transparency, and the integrity of the resulting record across the entire lifecycle of the change, rather than treating any single procedure as sufficient on its own.

The practical benefits of that redesign extend to every party involved:

- **Fund managers** gain stronger governance over one of their most sensitive operational processes while cutting unnecessary manual effort.
- **Administrators** spend more of their time on judgment and less on repetitive verification.
- **Investors** get more consistent, more transparent handling of changes to their own accounts.

The right test for any organization's investor change management, in the end, is not whether each individual control was completed, but whether the governance framework as a whole produces genuine confidence — a question best answered through periodic self-assessment against the principles set out here, rather than through a one-time compliance checklist.

8. CONCLUSION: BEYOND THE CALLBACK

The callback earned its place in private fund administration honestly. In an era when sensitive investor requests arrived almost exclusively through channels that could not be trusted on their own, independently verifying those requests was sound, disciplined practice, and it served the industry well for a very long time.

But the environment that made it indispensable has moved on. Secure authentication, identity management, governed workflows, and integrated platforms now make it possible to establish confidence in who is making a request before that request is ever accepted — something the industry simply could not do when the callback first became standard practice.

That capability does not just add a new tool to the toolkit; **it changes what governance is for.** Where investor change management once centered on determining whether a communication could be trusted, it should now center on ensuring that an authenticated request is governed appropriately from the moment it is initiated to the moment it becomes part of the permanent record — with identity, authority, oversight, transparency, and information integrity functioning as connected parts of one process rather than as separate administrative chores.

This is not an argument for eliminating callbacks, nor is it an argument for adopting any particular technology. It is a broader shift in how the industry should think about investor servicing, and it will not happen overnight. Many organizations will run hybrid processes for years, and there will continue to be circumstances where independent verification outside a digital channel remains the right call. Change in financial services rarely arrives all at once; it accumulates as technology matures, practices improve, and confidence builds in new approaches.

But the direction is not really in doubt. Organizations are moving away from processes that assume every communication must be verified from scratch, and toward models where trust is established before a sensitive request ever enters the governance process — and as that shift continues, investor change management will increasingly be judged not by any single control, but by the quality of the governance framework built around it.

Investor change management was never really about updating a record. It is about protecting investor assets, preserving confidence in sensitive information, and making sure that any significant decision affecting an investor can withstand scrutiny long after the fact. The callback was the industry's best answer to that challenge for a long time, and it deserves to be remembered as such.

Today's environment offers a different answer — one built on establishing trust before a request is accepted rather than after, so that governance can focus less on whether a message is genuine and more on whether every authenticated request is handled appropriately, transparently, and consistently across its full lifecycle. That is the shift this paper has tried to describe, and it is the sense in which the industry's task now lies beyond the callback.

The future of investor change management will not be defined by how organizations verify communications. It will be defined by how confidently they establish trust before those communications ever occur.
