Keeping the Tax Authority Record Straight

A practical change-control playbook for cross-border tax data, authorisations, representatives and evidence

Executive summary

Tax authority data is often viewed as a necessary administrative burden. Typically, a company registers, files a few forms, sets up portal access, maybe they appoint an agent or a fiscal representative, and then shifts focus to the regular cycle of compliance. This approach is understandable, but if information isn't governed correctly then it can carry significant risks (or at the very least additional administrative overhead later down the line).

The challenge is that tax authority records can quickly become outdated. As businesses expand, restructure, change directors, rotate finance teams, or replace third party compliance teams/software, records may not be updated accordingly. Changes to bank arrangements, registered offices, or treasury processes can also create gaps. Issues often go unnoticed until a notice is sent to the wrong contact, or a mandatory notification to the tax authority cannot be executed because of mis-aligned authorisations.

The recommendation from this white paper is straightforward: treat tax authority data, access, mandates, representatives, and evidence as controlled records. This adds process, and it also stops things consuming an in-ordinate amount of time and energy usually when you have the least to give. Cross-border compliance is too complex to run on memory, buried email chains, or last-minute heroics.

Learning from my background, IT governance and change-control principles are useful here. In IT, changes to production systems are managed with clear records of what changed, who approved it, potential risks, rollback plans, and supporting evidence. Many businesses make changes to tax-critical personnel, entities, providers, and processes without the same discipline. The result is usually incremental: outdated authority details, unclear authorisations, abandoned portal access, missing confirmations, unrevoked powers of attorney, and no definitive record of current authority information.

We're not defining country rules here - we're defining a control model. Notification requirements vary by jurisdiction, tax type, entity status, and representative relationship. The objective is to spot changes early, decide whether the authority record is affected, act before the issue becomes urgent, and keep evidence that the action was completed. The business should know who is authorised to act and be able to prove it.

Who this is for

- CFOs, finance directors, tax directors and shared services leaders managing filings and payments across multiple jurisdictions.
- Compliance partners, advisory firms and tax technology providers who support clients internationally and need a cleaner delivery model.
- Digital businesses, marketplaces, AI companies, and software-led groups are expanding faster than their back-office controls can keep up.
- Anyone who has ever said "the local agent has that" and then discovered that the local agent had left, merged, rebranded, retired, or decided not to answer emails on Fridays.

1. The hidden risk: the authority record quietly goes stale

I am starting with the vanilla version of the story. An organisation registers for VAT in several countries. It potentially appoints agents, nominates contacts, sets up portals, assigns internal owners, creates payment references and stores a few confirmation letters. It is not perfect, but it works. Then the business grows. New markets arrive. A bank account changes. Finance operations move from one team to another. A tax manager leaves. A change in compliance provider or software. A fiscal representative is replaced. An entity name changes after a restructure. The compliance calendar still exists, but the underlying authority record has started to drift away from operational reality.

That drift matters. The tax authority record is the set of facts, authorities and permissions that allow the business to file, pay, respond and prove. You often will not notice a stale record until something breaks
- usually a missed notice, a blocked portal login, an unrecognised payment, a provider handover, a market exit, or a director asking a perfectly reasonable question: “can someone show me the current list of authorised representatives?”

At that point, everyone learns the same lesson: doing something and proving it was done properly are not the same thing.

Plain-English definition

A tax authority change-control process is the discipline of knowing what authority-facing data exists, what changed, who is allowed to act, whether the authority needs to be told, and what evidence proves the record was updated.

2. Why does this look oddly like IT governance

My IT background and experience applying this to Tax means this looks a lot like IT governance. In information security, service management, and systems operations, you do not change a production system without thinking about dependencies, access, approvals, logs, backups, and rollback. Tax authority records deserve the same respect. Change the wrong contact, leave the wrong person with access, miss a mandate update, or lose the evidence trail, and the compliance workflow breaks in a very practical way.

ISO27001 is useful here because it forces a simple question: what information is critical, who can touch it, and what evidence shows it is controlled? ITIL makes the same practical point through change enablement. The goal is simple: low-risk changes happen quickly, high-risk ones are controlled. Whilst you don’t need to be an expert in these fields to understand the principles, I wanted to lean into proven frameworks to demonstrate the effectiveness and practical implementation.

Tax authority data is not a server, but it behaves like an operational dependency. It has owners, permissions, credentials, data fields, workflows, external parties, audit evidence, and consequences when it fails. The control model should be proportionate, practical, and efficient.

IT governance concept	Tax authority equivalent	Why it matters

IT governance concept	Tax authority equivalent	Why it matters
Configuration item	VAT registration, portal account, mandate, fiscal representative appointment, payment reference, notice address	You cannot control what you have not identified.
Access control	Portal users, agents, authorised representatives, payment approvers, MFA holders	Former users and informal access are a quiet risk.
Change request	Entity change, people change, provider change, bank change, market entry or exit	Every change should have an owner, reason, effective date and impact assessment.
CAB / change approval	Tax, finance, treasury, legal and operations review	Not every change needs a meeting. Some definitely do.
Audit log	Authority confirmations, screenshots, submitted forms, case numbers, approvals	If it isn't recorded, you won't be able to prove it.
Periodic access review	Annual portal and mandate review	The register only helps if it is kept alive.

3. The Porter angle: signals, not surprises

There is also a strategy angle here. Porter's competitive strategy work is famous for analysing industry structure and competitive forces, but one of the useful ideas we can utilize for tax is the concept of signals: observable events that tell you something has changed and that you should respond. In competitive strategy, those signals might be price moves, capacity expansion, new entrants, supplier behaviour or customer shifts. In tax operations, the signal is often more mundane but just as important.

A new sales channel. A new country. A new fulfilment route. A new banking provider. A new compliance partner. A new director. A new ERP. A new legal entity. A regulator changing a portal process. A customer contract requires local registration evidence. A bank refusing a payment format. A tax authority sending notices to an inbox nobody checks because it belonged to someone who now sells sourdough starter kits in Devon.

Your tax setup likely changes every time the business changes. Cross-border tax operations do not move only when tax law changes. They move when sales channels, entities, banks, providers, people, systems, and regulators change. A good control model needs signal detection, not just technical tax monitoring. This also doesn't need to require significant overhead and management, the proposal here is to tap into what you are likely already doing today but respond to the signals in near realtime.

Signal	What it may indicate	Review triggered
New market entry	New registration, representative, filing, payment and evidence requirements	Jurisdiction onboarding review
New customer segment or channel	VAT/GST, invoicing, marketplace, platform or digital services implications	Tax obligation and authority record review
Provider or agent change	Authority mandates, portal access and notice routing may be wrong	Representative and access review
Entity restructure or M&A	Registrations may no longer reflect the business	Entity and jurisdiction review
Banking or treasury change	Payment routes, bank details or approvals may change	Settlement control review
Key person or role change	Access, MFA, notices or approvals may be affected	Access and authority review
Authority portal update	Processes or credentials may stop working	Portal and evidence review
Audit, enquiry or notice	Records and controls may be tested	Evidence and contact review

4. The practical model: six things to control

In practice, this boils down to six things to monitor and control:

- Register what the authority-facing record contains – what have you told them and when.
- Control who can act, access, amend, file, pay and receive notices – ensure you maintain authority.
- Treat business changes as signals that the tax record may need review – regular pulse taking.
- Decide whether the tax authority, agent, fiscal representative or internal owner needs to be notified – create targeted action rather than noise.
- Evidence of what was requested, approved, submitted, confirmed and still pending – recording to make life easier later.
- Review the register on a schedule, not only when something has gone sideways – consistency and preparation.

4.1 Register: What does the authority think is true?

A tax jurisdiction data register sounds boring until someone needs it urgently.

The register should capture the authority-facing facts by country, entity and tax type. This is the source of truth that answers questions such as: where are we registered, who is the authority contact, who has access, who is appointed, what obligations exist, how do we pay, where do notices go, and what evidence do we hold?

COMPANION TOOL

Jurisdiction Register

Maintain a single source of truth for authority-facing registrations, portals, representatives, payment routes, owners and review dates.

Included in this guide: The core fields, control purpose and practical role of the register.

Download the editable Jurisdiction Register

Record area	What to capture	Example of the problem if ignored
Entity data	Legal and trading name, tax ID, registered and correspondence addresses, establishment status	Outdated addresses can send notices to the wrong place.
Tax registrations	VAT/GST, corporate tax, payroll, withholding and customs registrations; filing frequency	A registration may appear dormant while returns remain due.
Authority portals	Portal, URL, users, access method, MFA owner and backup user	Access can fail when one former employee owns MFA.

Record area	What to capture	Example of the problem if ignored
Internal users	People who can view, file, amend, approve, pay or receive notices	Users may retain access after their role changes.
External users	Agents, advisers, fiscal representatives, filing and payment providers	A former provider may still hold authority.
Mandates and authorisations	POA, agent authority, fiscal representation agreement, portal mandate and revocation evidence	A provider may be unable to act if authority is incomplete.
Payment data	Payment route, payer, references, bank or direct debit details, refund account and approvals	Incorrect details can delay or misallocate payments.
Notice handling	Authority email, postal address, portal inbox owner and escalation route	Notices can remain unread without a clear owner.
Evidence	Returns, confirmations, screenshots, letters, forms, case numbers and change log	The business may act correctly but struggle to prove it.

4.2 Control: Access is not the same as authority

A common risk we see relates to Access, and often the access to perform the tasks needed – not the regular filing but to notify of changes. Access can be accidental, excessive, outdated, or informal.
Authority should be intentional, clearly defined, documented, and revocable. It is worth noting that some tax authorities require the authorisation to match the organisations articles of association, ensuring that the authorized individual has sufficient mandate.

In tax operations, this distinction matters. A person may have portal credentials but no current approval to file. An agent may have a mandate for one tax but not another. A fiscal representative may be formally appointed in one country and informally copied on emails in another. A finance team may approve payments internally but have no visibility of whether the authority record still points to the old bank or contact. These are not conceptual gaps; they are the everyday messiness of cross-border growth.

Authority type	Control question	Minimum record
Filing access	Who can submit returns, and for which taxes?	Named user, tax type, jurisdiction, approval basis and backup
Payment authority	Who can initiate, approve and evidence payments?	Approver matrix, limits, references and evidence owner
Portal access	Who can log in, amend details, retrieve notices or manage users?	User list, access level, MFA owner and review date
Representative authority	Who can act for the business?	POA or agent authority, scope, effective date and revocation process
Fiscal representative	Who holds the formal local role and liability?	Appointment, scope, jurisdiction, liability period and release evidence
Notice handling	Who receives, triages and escalates communications?	Inbox or postal route, owner, response target and escalation
Data amendments	Who can change registered details, bank data, contacts or mandates?	Requester, approver, approval rules and authority confirmation

4.3 Signal: What changes should trigger review?

The signal stage does most of the useful work. Not every change requires notifying a tax authority, but every relevant change should prompt a review at the very least. A good control model sends the right changes to the right owners without turning every address update into a crisis meeting.

The following signal matrix is designed to help determine which function—tax, finance, treasury, legal, operations, agent, or fiscal representative—should address a given change. It is not intended to be exhaustive but to be used and applied to your organisations specific requirements.

COMPANION TOOL

Change Intake & Trigger Assessment

Capture a business change while the context is still clear, then screen whether authority-record review or further assessment is required.

Included in this guide: The trigger categories, workflow logic and Appendix A one-page checklist.

[Download the editable Change Intake & Trigger Assessment]

Change signal	What to review	Possible authority impact
Legal entity name change	Registrations, invoices, portals, mandates and certificates	Authority records may need updating; retain evidence.
Address change	Registrations, notice routes, local requirements and portals	Authorities may need notification; notices may go astray.
Director or responsible person change	KYC, responsible-person records, agent and fiscal representative files	Some authorities may require an update.
Tax lead leaves	Portal access, MFA, notice routing, calendars and open cases	Access and escalation controls may need updating.
Finance approver changes	Payment workflow, limits, evidence ownership and delegated authority	May affect direct debit, payer validation or authority records.
Agent or adviser change	POA, portal access, notices and handover evidence	Old authority may need revocation; new authority may be required.
Fiscal representative change	Appointment, liability period, final filings and release evidence	High-risk transition requiring controlled handover.

Change signal	What to review	Possible authority impact
Bank or payment change	Direct debit, refund bank, payer details, references and settlement calendar	May require authority updates and payment-control review.
Platform change	Data fields, submission process, evidence archive, access and audit trail	Processes and evidence may change even if registrations do not.
M&A, restructure or branch change	Entity map, registrations, portals, mandates, payment routes and representatives	Often triggers several reviews and notifications.
Market exit or deregistration	Final returns, payments, notices, representative release and record retention	Usually authority-facing; evidence remains important after exit.

4.4 Notify: When does the authority need to know?

In most cases, it is likely - you'll need to update the authority record. The next question is often how. Notification requirements vary by jurisdiction, tax type, registration status, business activity and representative relationship. Sometimes that means a portal update. Sometimes it means a form, a new mandate, a fiscal representative change, or formal evidence that nothing further is required. In the some cases it could require a board level document.

The control question should be: does this change affect a record, permission, obligation, contact route, payment route, representative role or evidence trail that the authority relies on? If yes, the business should assess whether an official notification, portal update, agent mandate, POA amendment, fiscal representative update or supporting evidence is required.

External examples illustrate this point. HMRC guidance explains how organisations can revoke or remove a tax agent's authorisation and notes that the process varies by tax type. HMRC also advises against sharing sign-in credentials with agents. The IRS uses Form 8822-B for business taxpayers to report changes of address, business location, or responsible party, and Form 2848 to authorise an eligible individual to represent a taxpayer before the IRS. While the details differ, the operational lesson is clear: authority-facing data and the authority to act are formal matters and should be managed accordingly.

4.5 Evidence: if it is not recorded, it did not really happen

Evidence usually becomes important at the least convenient moment. It is not only for audits. It matters during handovers, provider changes, board questions, payment disputes, authority requests, acquisitions, and any situation where the person who "knows where it is" has left.

COMPANION TOOL

Evidence Checklist

Organise approvals, submissions, mandates, confirmations, screenshots, references and open issues before a change is closed.

Included in this guide: The evidence principle and closure requirements that make the audit trail usable.

Download the editable Evidence Checklist

Evidence item	What to retain	Why
Change request	Requester, reason, date, affected entities, jurisdictions and taxes	Explains why the change began.
Impact assessment	Affected registrations, portals, users, representatives, payments and notices	Shows the consequences were considered.
Internal approval	Approver, date, authority, conditions and effective date	Shows the change was authorised.
Authority submission	Forms, portal receipts, emails, letters and case references	Shows the authority-facing action occurred.

Evidence item	What to retain	Why
Mandate record	POA, agent authority, fiscal representative appointment, revocation and dates	Shows who could act and when.
Access log	Users added or removed, MFA changes, credential handover and review date	Shows access was controlled.
Confirmation	Authority acknowledgement, updated extract, screenshot or certificate	Shows the change was accepted or recorded.
Open issue log	Pending response, workaround, owner, next action and due date	Keeps unresolved risk visible.

4.6 Review: the register must breathe

A register that is created but never reviewed quickly becomes obsolete. The control model requires both routine and signal-based reviews. Scheduled reviews identify gradual changes, while signal-based reviews address recent changes while details are still clear.

Control	Suggested frequency	Owner
Portal user access review	Bi-Annual	Tax operations / finance operations
Agent and representative register review	Annually	Tax / legal / partnerships
Notice routing review	Quarterly	Tax operations
Bank and payment data review	Semi-annually	Treasury / finance operations
POA and mandate review	Annually	Tax / legal
Fiscal representative status review	Annually	Tax / compliance owner
Full jurisdiction register review	Annually	Global tax / finance operations
Joiner-mover-leaver authority access check	Every people change	HR / IT / tax operations
Provider change review	Every provider transition	Procurement / tax / operations
Entity restructure review	Every corporate change	Legal / tax / finance

5. Examples: where this goes wrong in real life

The following examples are anonymised and generalised. Most compliance failures begin with routine business changes that are not properly reflected in the tax authority record, rather than dramatic events.

Example 1: The ex-employee with the magic portal key

A finance manager leaves the company. Internal access to the ERP, banking platform, and email is removed as part of the standard offboarding process. However, overseas tax portals are not checked. Six months later, a filing issue arises, and the team discovers that portal multi-factor authentication is still linked to the former employee's phone number. Resolving this is possible but time-consuming, and the issue often surfaces at critical moments.

Control lesson: tax portal access should sit inside the leaver process, not in a separate clean-up exercise that starts after something fails.

Example 2: The agent change that only changed in Outlook

The business replaces a local adviser. While the old adviser is no longer involved and the new adviser is included in correspondence, the old agent mandate is not formally revoked, and the new authority is not properly recorded. As a result, a notice is sent to the previous contact, and the new adviser cannot access the authority account.

Control lesson: Changing who is copied on an email is not the same as changing authority.

Example 3: The fiscal representative handover with a long tail

A fiscal representative relationship is terminated in one country. The business assumes the termination is effective from the commercial end date. However, the local authority record, final filings, liability period, release evidence, and new representative appointment all require attention. The operational risk arises during the transition period between the end of the old responsibility, the start of the new responsibility, and formal authority recognition.

Control lesson: fiscal representative changes should be managed as controlled transitions, with defined effective dates and evidence packs.

Example 4: The bank change that looks like treasury admin

Treasury or AP centralises payment execution, which is commercially logical. However, this changes who initiates tax payments, which bank accounts are used, how references are generated, and who maintains supporting evidence. In some jurisdictions, direct debit or refund bank data may require updating. In others, the risk involves payment reference quality and reconciliation.

Control lesson: tax settlement is part of the compliance record. Payment changes should trigger authority and evidence review, not just banking implementation.

Example 5: The acquisition with inherited ghosts

A group acquires a business with existing registrations, agents, and portal accounts. After the deal closes, the clean-up starts. Some registrations are active, others are dormant, and some are managed by local accountants. Nobody is completely sure where notices go. That is why mergers and acquisitions should trigger a full review of the tax authority register.

Control lesson: inherited registrations are inherited controls. If you do not review them, you own any gaps they create.

6. The minimum viable control pack

For organisations seeking a practical starting point, avoid lengthy policies that are difficult to maintain and rarely read. The first public release is built around three practical companion tools, supported by additional controls as the operating model matures:

- Core tool 1 — Jurisdiction Register: a single source of truth for registrations, portals, mandates, representatives, notices, payment routes, owners and evidence.
- Core tool 2 — Change Intake & Trigger Assessment: a combined workflow to capture what changed and screen the review actions that should follow.
- Core tool 3 — Evidence Checklist: an evidence library and close-out checklist for requests, approvals, submissions, mandates, confirmations, screenshots and open issues.
- Advanced control — Impact Assessment Framework: use for complex, multi-jurisdiction, representative, banking or systems changes.
- Additional control — periodic access and representative reviews may be added where the operating model requires more depth.
- Additional control — maintain a consistent evidence folder structure by entity, jurisdiction, tax type and event.
- Governance support — retain the RACI in this guide and adapt it to the organisation’s actual operating model.

Public companion tool	What appears in the guide	Editable download
Jurisdiction Register	Purpose, core fields and use within the control model.	Excel workbook
Change Intake & Trigger Assessment	Capture-and-screen workflow, trigger categories and Appendix A.	Editable Word form
Evidence Checklist	Evidence principle, categories and close-out requirements.	Excel workbook

Template	Purpose	Key fields
Jurisdiction register	Source of truth for authority-facing records	Entity, country, tax type, ID, portal, contacts, obligations, payments and evidence
Change intake form	Capture the signal before it is lost	Requester, change type, date, countries, tax types, urgency and owner
Impact assessment	Map the consequences of the change	Registrations, access, mandates, notices, payments, filings and providers
Authority notification log	Track authority-facing action	Channel, date, reference, owner, confirmation and status

Template	Purpose	Key fields
Access review sheet	Remove stale or excessive access	User, role, portal, MFA, last login and keep/remove decision
Evidence checklist	Make proof easy to find	Request, approval, submission, mandate, confirmation and open issue

7. A practical workflow

Keep the workflow simple. Over-engineered processes die in inboxes. The controls that work are the ones people can actually follow (and remember to follow when the time comes).

1. Spot the signal. Something has changed: a person, entity, market, provider, bank route, platform, authority process or obligation.

2. Open a change record. Use the Change Intake section of the editable Change Intake & Trigger Assessment to capture essential details before information is dispersed through informal email chains.
3. Map affected jurisdictions. Use or update the Jurisdiction Register to identify which countries, tax types, portals, mandates, representatives and payment routes could be affected.
4. Classify the risk. Complete the Trigger Assessment. For complex or high-risk changes, use the Impact Assessment Framework before deciding authority-facing action.
5. Assign owners. Tax owns tax positions; finance owns settlement controls; treasury owns bank flows; legal owns entity and mandate issues; IT supports access and identity control; providers own what they are contractually appointed to do.
6. Decide notification/action. Confirm whether an authority update, portal amendment, mandate change, representative update, access change or evidence capture is needed.
7. Execute and evidence. Submit forms, update portals, revoke old access, appoint new authority, store confirmations, and record the supporting evidence in the Evidence Checklist.
8. Close or monitor. Close only when confirmation is received or when a named owner is tracking the open authority response. Confirm that the Evidence Checklist is complete.

8. Suggested RACI

R = responsible, A = accountable, C = consulted, I = informed. The appropriate RACI is the one that aligns with the actual operating model, rather than simply appearing organised in documentation.

Activity	Tax	Finance Ops	Treasury	Legal	IT / Security	External provider
Maintain jurisdiction register	A/R	R	C	C	C	C
Assess tax authority notification requirement	A/R	C	C	C	I	C
Remove portal access for leavers	C	C	I	I	A/R	C
Update payment routes and evidence	C	R	A/R	I	C	C
Manage POA / agent mandate	A/R	C	I	C	I	R where appointed
Manage fiscal representative change	A/R	C	C	C	I	R where appointed

Activity	Tax	Finance Ops	Treasury	Legal	IT / Security	External provider
Retain authority confirmations and evidence	A	R	R for payments	C	C	R for provider actions
Quarterly access review	C	C	I	I	A/R	C

9. What this means for Desucla clients and partners

The commercial point is clear. Cross-border tax compliance is not simply about knowing the rules. It is about being able to execute the rule repeatedly across countries, entities, people, providers, payment routes and authority systems.

Many businesses struggle here. They ask for "compliance" and end up with activities spread across local agents, tax teams, treasury, finance operations, technology platforms and inboxes. The tax authority change-control model exposes the operational layer: what exists, who can act, what changed, what needs review, what was notified and what evidence proves it.

For partners, this model is valuable because it enables structured delivery discussions. Partners do not need to develop every local capability internally, but they must understand how authority-facing records, mandates, access, and evidence will be managed as clients expand or change. A coordinated execution partner plays a key role by ensuring these essential processes function reliably.

10. Final thought: the boring controls are the ones that save you

Maintaining an up-to-date tax authority register is not glamorous. No one is putting it on a conference lanyard. But it is one of the controls that prevents painful, avoidable failures.

Operational control separates a scalable compliance model from a collection of disjointed activities. As businesses expand across jurisdictions, success depends not only on understanding VAT, GST, withholding, customs, or payment rules. It also depends on managing the authority-facing facts and authorisations that make compliance possible.

The tax authority record should be transparent, with clear ownership, regular review, timely updates, and documented evidence. The business should know who is authorised to act, who previously held authority, who receives notices, who approves payments, which representative is appointed, which changes are pending, and where supporting documentation is stored.

From my experience most teams don't do this consistently. The businesses that do are usually the ones that identify signals early, update the authority record before it becomes urgent, and can prove what happened when someone asks.

Appendix A: One-page change trigger checklist

Question	Yes/No	Action

Question	Yes/No	Action
Has the legal entity name, address, responsible person, director or ownership changed?		Review registrations and notification requirements.
Has a tax, finance, treasury or compliance owner joined, moved or left?		Review portal access, MFA, notice routing and approvals.
Has an external agent, adviser, provider or fiscal representative changed?		Review mandates, portal access, revocation, appointment and evidence.
Has a bank account, payment route, direct debit or refund account changed?		Review payment records, references, bank details and evidence.
Has the business entered or exited a jurisdiction?		Review registrations, final returns, representatives, payments and retention.
Has the ERP, tax engine, filing platform or payment platform changed?		Review data flows, access, audit trail and evidence.
Has an authority portal, process, form or digital requirement changed?		Review process documentation and ownership.
Has an audit, enquiry, notice or dispute been received?		Review evidence, notice routing and authority contacts.