ACCCF / Applied Knowledge Library

10

VOLUME

Reconciliation, material performance and authentication records

Spanish edition · 2026

Financial Forensics and Documentary Contradiction Manual: Banks, XML and SAT

CFDI, bank statements, transfers, references, timelines and contradictions

Reconstruct transactions using verifiable documents and records, without confusing an invoice with the underlying transaction, a transfer with its purpose, or successful authentication with consent.

For forensic experts, accountants, lawyers, auditors, fraud, compliance and management teams. Tax interpretation and legal liability depend on the applicable regime, date and case file; this manual does not offer strategies to conceal transactions or evade obligations.

Editorial coordination: Jocsan Laguna · American Council for Cybersecurity and Forensic Computing

General technical guide and open educational material. It does not constitute legal advice, an expert opinion, or instructions for accessing systems without authorization. Examples and data are fictitious; figures are editorial reconstructions.

Contents

Visible page numbers correspond to the PDF edition. Word may update this table of contents when the document is opened; headings retain internal navigation.

Introduction: documents speak more clearly when asked questions 3

Chapter 1. Question, period and sources 3

- **1.1 Separate statements and unit of analysis** 3
- **1.2 Source inventory and authority** 4

Chapter 2. Reconciliation 4

- **2.1 The chain of correspondence** 4
- **2.2 Differences and documented explanation** 4
- **2.3 Example of a remittance and credits** 5

Chapter 3. XML and representations 5

- **3.1 XML as a structured source** 5
- **3.2 Folio, duplication and material performance** 6
- **3.3 Metadata, representations and dates** 6

Chapter 4. Bank records and financial chronology 7

- **4.1 The transaction in its sequence** 7
- **4.2 Supporting documents and provider records** 7
- **4.3 Financial rules and their scope** 7

Chapter 5. Unrecognized transactions 8

- **5.1 Enrollment and factor control** 8
- **5.2 Security signals and system behavior** 8
- **5.3 Authentication and authorization matrix** 9

Chapter 6. Documentary contradiction report 9

- **6.1 Separating observation, reconciliation and inference** 9
- **6.2 Chronology and limitations** 10
- **6.3 Independent review** 10

Annex A. Reconciliation and request formats 10

- **A.1 Reconciliation matrix** 10
- **A.2 Request for financial records** 11
- **A.3 Unrecognized transaction matrix** 11

Annex B. Comparative documentary framework and final review 11

Introduction: documents speak more clearly when asked questions

An invoice may look perfect and still not prove that the goods were delivered. A transfer may exist without explaining its purpose. A bank statement may match the accounting records and still leave unanswered who authorized a transaction. Financial analysis does not mean choosing the document that looks most official; it means following the chain from contract, supporting document and material performance to bank transaction, records and accounting.

The forensic examination starts with a specific allegation: nonexistent transactions, duplication, payments not received, unrecognized transfers, balances that do not match, or activity inconsistent with the reported transaction. It then identifies which source can confirm or weaken each allegation. Matching amounts help locate candidates, but alone do not prove a relationship or intent.

The work separates four dimensions: documentary form, material reality, the money trail, and system behavior. The first reviews XML, PDF, seals, folios, and versions; the second, delivery, personnel, assets, and independent evidence; the third, accounts, references, and settlement; the fourth, enrollment, factors, alerts, and behavior. A responsible conclusion does not blur these dimensions to resolve them with a single date.

> **Guiding rule**
> The existence of a document and the truthfulness of the transaction are related but distinct questions. Each requires its own source and method.

Chapter 1. Question, period and sources

1.1 Separate statements and unit of analysis

Record each party's allegations with dates, amounts, accounts, references, and transactions, without accepting the account as fact. A merchant may claim unsettled sales; the processor may say it did not receive them; the bank may show partial credits. The unit of analysis may be a transaction, batch, remittance, invoice, transfer, or business day. Choose it before adding amounts to avoid mixing levels.

Define the period and time zone, currency, taxes, fees, refunds, chargebacks, exchange rates, and rounding. Differences may result from a fee, settlement calendar, or incomplete file, not automatically fraud. Tolerances must be justified by business rules and documented; they must not be adjusted until the result looks convenient.

Question	Priority sources	Do not confuse with
Was the transaction recorded?	Business system, CFDI, purchase order and accounting records.	Material existence of the good or service.
Was it delivered?	Receipt, logistics, performance and independent evidence.	Tax folio or written description.
Was it transmitted?	Remittance, processor, interface and records.	Capture of the final report.
Was it settled?	Bank, reference, batch and calendar.	Treating matching amounts as unique identification.

Question	Priority sources	Do not confuse with
Was it authorized?	Factors, sessions, alerts, contract and context.	A system “yes” as human consent.
What was left out?	Filters, period, channels and missing documents.	Absence from a file as universal nonexistence.

1.2 Source inventory and authority

The inventory includes contracts, purchase orders, XML and PDF, bank statement representations, bank files, processor records, interfaces, accounting records, inventories, logistics, communications, and personnel. Each source has a custodian, format, period, coverage, and authority. Requests for personal or financial information must be limited to the relevant transaction and use a secure channel.

Do not request “the entire bank” or “the entire SAT.” Request transactions by reference and period, available native format, data dictionary, extraction process, filters, and a coverage statement. Preserve the delivery with EML and attachments. If a provider supplies a hash, verify it; if not, calculate one upon receipt and document its scope.

> **Starting condition**
> Before adding amounts, verify which transaction each row represents and which document supports each allegation. Accounting cannot be reconciled by adding totals without identity and coverage.

Chapter 2. Reconciliation

2.1 The chain of correspondence

Create one row per transaction and link the purchase order, CFDI, delivery, remittance, processor, bank, and journal entry. Do not fill missing fields with assumptions. If an invoice has no associated bank transaction, mark it pending; if there are two candidate transactions, describe the alternatives and the evidence needed. The goal is to show where the chain breaks, not to force every row to match.

The relationship may be one-to-one, one-to-many, or many-to-one. A batch may group sales; one transfer may cover several invoices; a refund may affect only part. The method must state how a transaction is allocated and avoid assigning amounts twice. Compare totals at each level with the source to detect duplication or missing records.

2.2 Differences and documented explanation

Fictitious discrepancy	Checks	Provisional conclusion
Same amount on two different dates	Reference, originator, account, channel and payment description.	Possible candidate; identity not confirmed.
Invoice with no matching credit	Calendar, batch, fees, refund and another account.	Pending or explained, depending on the source.
Credit without an invoice	Earlier charge, advance payment, later relationship or error.	Do not assign it just to balance the totals.
Short remittance	Filters, transmission, duplicate batch and cutoff time.	Coverage before allegations.
Different balance	Currency, taxes, rounding and commissions.	Quantified and explained discrepancy.

Fictitious discrepancy	Checks	Provisional conclusion
Duplicate document	UUID, folio, file, hash and representation.	Actual duplication or two copies of the same object.

2.3 Example of a remittance and credits

A fictitious store reports 18,420 transactions over three days. Its file contains that many rows, but one remittance contains only 17,900. The first question is not who stole, but whether the cutoff time, filters, or channel excluded events. Compare source, transmission, processor, and bank files using time zones and calendars. A later credit may belong to a different batch; do not use it to close the discrepancy without establishing a relationship.

If an export confirms that the missing references were not transmitted by the store, the finding points to its generation process. It does not yet establish a cause or responsible party. Possibilities include an unrecorded transaction, filtering, failure, or duplication. The report separates absence from the remittance, existence at the point of sale, and the bank credit, and proposes the next source that can distinguish among these hypotheses.

Reconciliation result

A matrix showing correspondence, discrepancies, duplication, omissions, and outstanding questions. The totals are a check; the explanation is the analysis.

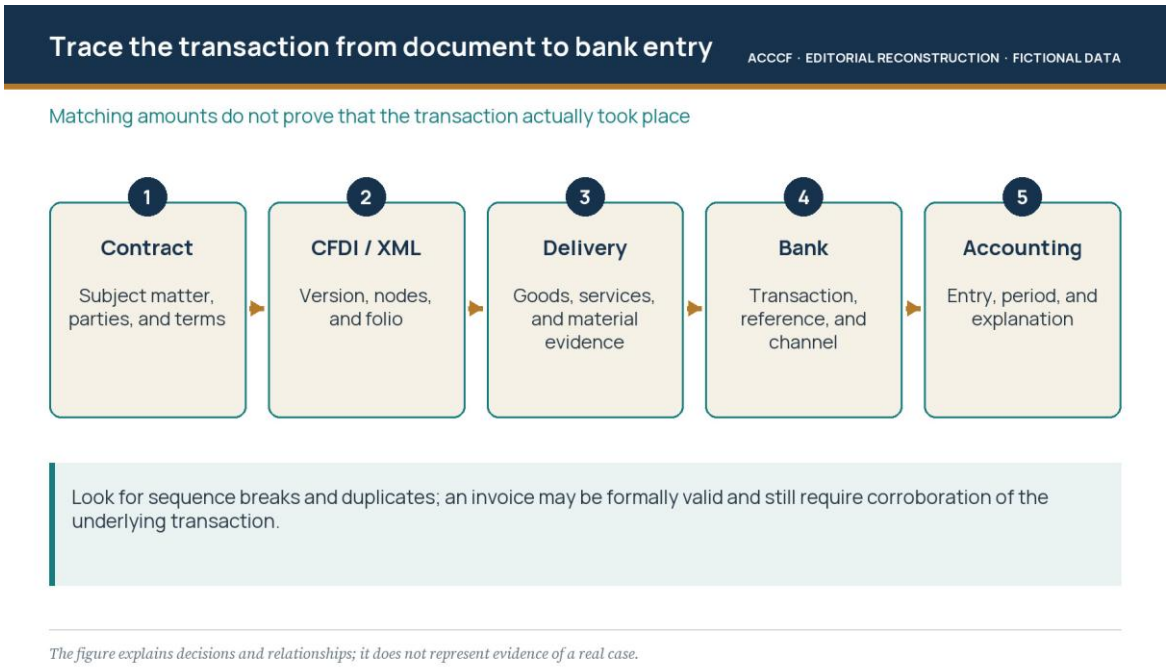


Figure 1. The transaction is traced from document to bank entry. Matching amounts do not prove material performance. Editorial reconstruction; not actual evidence.

Chapter 3. XML and representations

3.1 XML as a structured source

XML preserves nodes, attributes, and relationships that a PDF representation may not show. Preserve the original file with its name, size, receipt date, and hash, and analyze a copy. Review the version, issuer, recipient, folio, type, currency, line items, taxes, complements, and related documents as required by the engagement. Do not modify the file to “see whether it validates.”

Official SAT material provides completion guides for CFDI 4.0 and complements. The selected guide must match the document type and date. Attributes may change between versions; do not compare a historical XML file with an example from another version as if they were identical. PDF supports reading; XML supports structural analysis.[1]

3.2 Folio, duplication and material performance

The UUID helps identify a receipt, but duplication must be assessed using the file, structure, issuer, folio, amount, and context. Two identical files may be copies of the same object; two different XML files with the same UUID require clarification. A seal or digital stamp alone does not prove delivery of goods or provision of a service.

Material performance is reviewed using the contract, purchase order, inventories, delivery, performance records, personnel, communications, access logs, and independent evidence. The question is not only whether the CFDI is formally correct, but whether the described activity is supported. The analysis does not automatically declare a crime or sham transaction: it identifies which documents agree, which facts are missing, and which contradictions exist.

3.3 Metadata, representations and dates

The CFDI issue date is not necessarily the delivery, payment, or accounting date. The file's system date may be the download date. The PDF representation may show a different version if generated from another XML file. Link the objects and preserve every version. A hash establishes integrity from receipt, not the reality of the transaction.

Object	What it proves	What requires another source
XML received	Structure and content of the file in that delivery.	Authenticity of the transaction and full coverage.
Associated PDF	Declared visual representation.	That it comes from the same XML without comparison.
UUID	Receipt identifier.	That there is no error, duplication or sham transaction.
Delivery	Evidence of goods or services.	That all invoices represent actual transactions.
Hash	Object equality at a specific point in time.	Date, authorship and economic reality.

Fictitious case

Two XML files have the same UUID but different descriptions. Do not choose the one that favors a party: preserve both, request the issuer's records, history, and relevant verification, and compare them with delivery and accounting records. The content discrepancy must be explained before attributing a transaction.

[1] SAT. Invoicing guidance: completion guides for CFDI version 4.0 and complements. XML must be analyzed using its applicable nodes, catalogs, and version; PDF is a visual representation, not a substitute for the structured document. Official online source

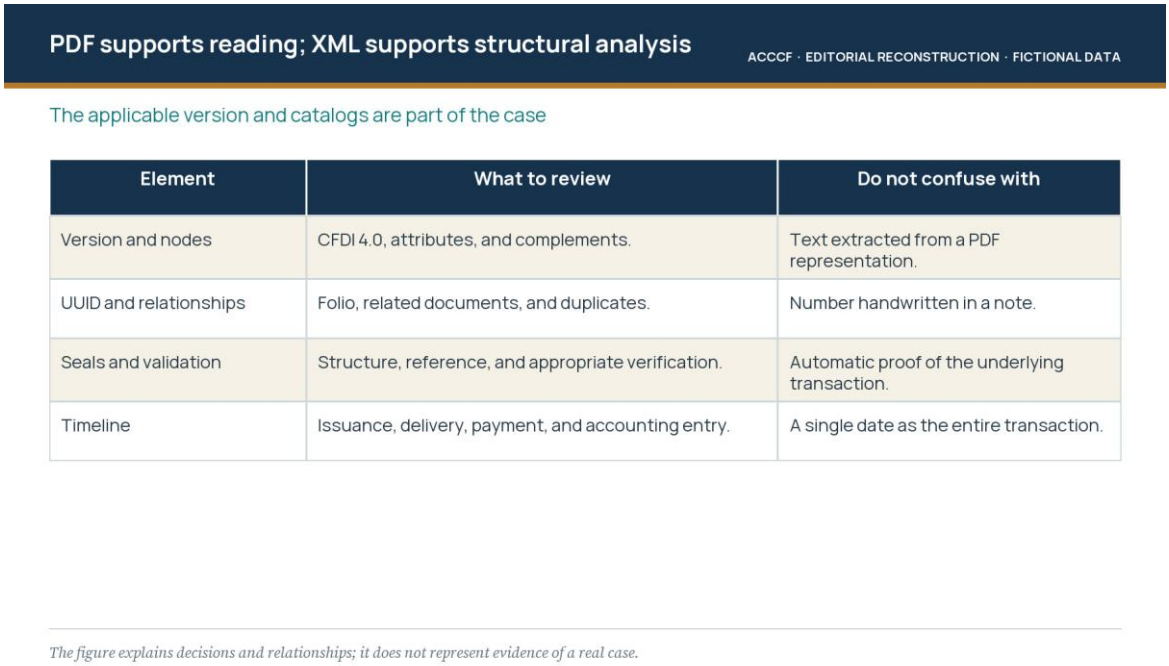


Figure 2. PDF supports reading; XML supports structural analysis. The applicable version and catalogs are part of the case. Editorial reconstruction; not actual evidence.

Chapter 4. Bank records and financial chronology

4.1 The transaction in its sequence

The bank statement identifies the date, time when available, amount, currency, reference, originator, beneficiary, channel, and balance. Request the fields and data dictionary. A transfer may have different instruction, execution, clearing, and availability dates. Do not merge them into one chronology column. The credit's existence does not prove which contract caused it or who ordered it.

Reconstruct the sequence from instruction to settlement using supporting documents, alerts, rejections, refunds, chargebacks, and channel records. If an account is blocked or frozen, request the relevant order, scope, date, and related transactions through legal channels; do not try alternative access methods. No activity in one account does not prove no activity in others.

4.2 Supporting documents and provider records

A visual receipt must be linked to the provider's record, not to an isolated screenshot. Request the native export, data dictionary, process, and coverage. If a reference or folio exists, use it to establish a link, not to replace validation. An image saying “transfer successful” may indicate an instruction, not final receipt or account authenticity.

The provider's delivery EML preserves the integrity statement and attachments. The hashes of the EML, report, and system are distinct objects. If the provider supplies only PDF, request CSV or native format for structural analysis; if unavailable, state the limitation and work with the received representation without presenting it as the complete database.

4.3 Financial rules and their scope

In Mexico, CNBV provisions cover supporting documents, notifications, access, incidents, operational incidents, logs, and reviews for credit institutions. In Peru, SBS 504-2021 regulates preservation and forensic analysis at supervised entities, and SBS 2286-2024 amends certain cases involving unrecognized transactions. In Spain, RD-ley 19/2018 regulates restitution subject to conditions and exceptions. These

rules do not mean that every authentication proves authorization or that every bank responds in the same way.[2345]

Jurisdiction	Useful sector-specific source	Caution
Mexico	CNBV 316 Bis 11, 14, 15 and 17 for access, incidents, logs and review.	Scope and time limits differ by article.
Peru	SBS 504-2021 and 2286-2024 for preservation, records and certain transactions.	Read the applicable cases and exceptions; do not generalize liability.
Argentina	BCRA A 7783 and A 8280 for records and incidents.	90 days of digital records and reporting under its own regime, not universally.
Chile	RAN 20-7, 20-8 and 20-10 for outsourcing, incidents and cybersecurity.	Do not confuse functions or regulated entities.
Spain	RD-ley 19/2018, 45, 66 and 67.	Conditional restitution and incident management/notification.

Interpretation rule

The bank record proves what the system recorded. Legal authorization and the originator's identity require additional analysis.

Chapter 5. Unrecognized transactions

5.1 Enrollment and factor control

Review who enrolled the device or factor, using which method, date, channel, and evidence; subsequent changes; recovery; deactivation; alerts; and access. A second factor can reduce risk, but does not prove that the account holder approved every transaction if enrollment was compromised or recovery was the attack path. The sequence begins before the transfer.

NIST SP 800-63B-4 distinguishes assurance levels and addresses phishing-resistant authentication. The guide does not support concluding that all MFA is equivalent or that recovery is a secondary detail. The analysis considers channel, domain binding, device, session, and phishing exposure. Technical claims are limited to what the source establishes.[6]

5.2 Security signals and system behavior

Review alerts, rules, new devices, beneficiary changes, approximate location, amount, frequency, prior behavior, and the bank's response. A transaction may be blocked by the system and later allowed through an alternate channel. The absence of an alert does not prove the transaction was normal; it may result from configuration or coverage.

Compare recognized and unrecognized transactions without bias. If the recognized transactions share a device and pattern with the unrecognized ones, attribution may be consistent with habitual use or with a

[2]General provisions applicable to credit institutions, Articles 316 Bis, 316 Bis 1, and 316 Bis 10 to 17: supporting documents, encryption, access, incidents, operational incidents, logs, and reviews. Official online source

[3]Peru. SBS 504-2021, Articles 12.6.g, 15 and 17.3–17.4: preservation, reporting and forensic analysis, records of enrollment, authentication and transactions. Official online source

[4]Peru. SBS 2286-2024: amendment to Article 20.3 on certain unrecognized transactions and liability, unless the user's liability is proven. Official online source

[5]Spain. Royal Decree-Law 19/2018, Articles 45, 66 and 67: restitution for unauthorized transactions, risk management, and immediate notification of serious incidents. Official online source

[6]NIST SP 800-63B-4 (July 2025). Guidelines for authentication and authenticator management, including assurance levels and phishing-resistant authentication. Account recovery is part of the risk and must not be reduced to passwords. Official online source

persistently compromised account. If a factor changes minutes earlier, investigate its origin. Do not base the conclusion on the phrase “the system validated correctly.”

5.3 Authentication and authorization matrix

Element	What it establishes	Outstanding question
Enrollment	Factor record and date.	Who started it and with what control?
Authentication	The system accepted factors at an event.	Were they the account holder's factors, and how were they recovered?
Alert	The system classified a condition.	What action did it take, and with what result?
Transaction	Instruction and result on the channel.	Was there consent and what contract applies?
Account holder	Account and contractual relationship.	Who was using the channel at the time?
Liability	Rule and established facts.	Which case and exception apply?

Fictitious case

An unrecognized transfer follows a recovery email change and enrollment of a new device. The bank recorded valid authentication, but that sequence requires review of the earlier change. The analysis does not allege fraud by the account holder or automatic bank liability: it documents the events and the applicable rule.

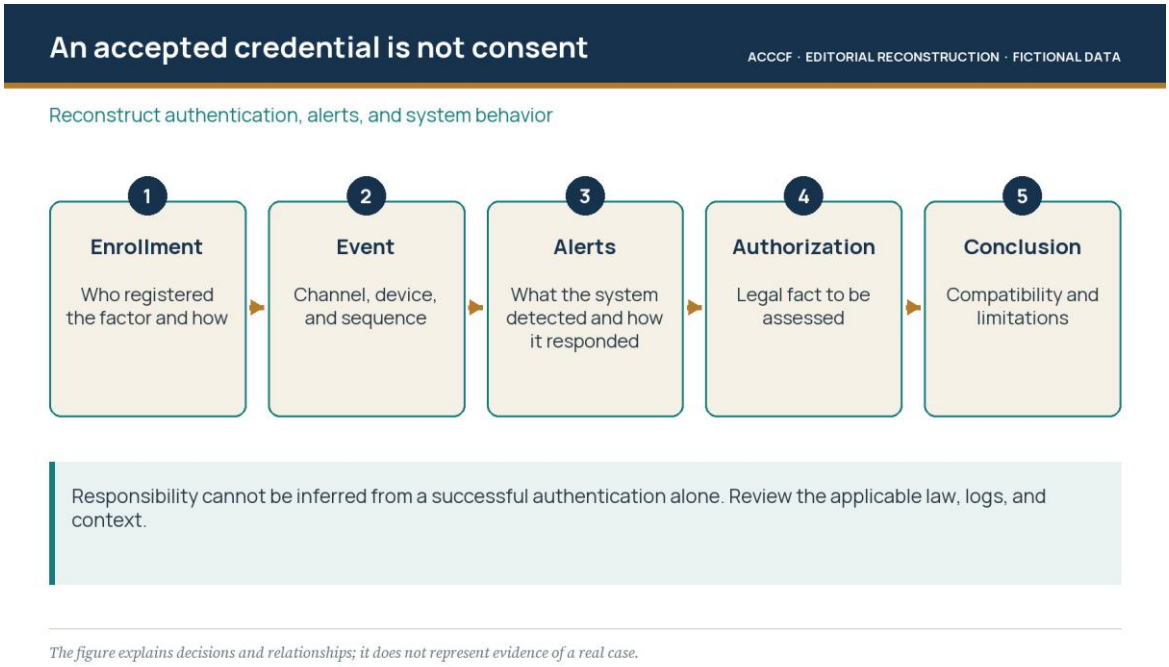


Figure 3. An accepted credential does not equal consent. Authentication, alerts, and system behavior are reconstructed. Editorial reconstruction; not actual evidence.

Chapter 6. Documentary contradiction report

6.1 Separating observation, reconciliation and inference

The report distinguishes what the file contains, what reconciliation produces, and what the analyst interprets. “The XML contains this amount” is an observation; “the candidate entry matches the amount

and reference" is reconciliation; "it is consistent with the reported transaction" is an inference. Liability or legality is a separate question that must not be hidden among the totals.

Each discrepancy has a section with literal values, sources, alternative explanations, result, and outstanding need. It is not removed because it complicates the narrative. If a transaction cannot be linked, mark it undetermined. If a new source changes the relationship, update the matrix and preserve the previous version.

6.2 Chronology and limitations

The chronology preserves issuance, delivery, transmission, instruction, settlement, accounting entry, and communication, with time zone and precision. Proximity between two events does not prove causation. Missing events outside the export must not be used to claim nonexistence. The report identifies channels and accounts not reviewed.

Statement	Defensible wording	Limit
Matching amount	Compatible candidate by amount, reference and period.	No unique identification without other sources.
Invoice without a transaction	No material evidence was found in the scope reviewed.	Do not claim a complete sham without coverage.
Unrecognized transfer	Instruction and authentication were documented in the channel.	No automatic inference of human consent.
Duplicate document	The objects share UUID and present these differences.	Do not delete either object or choose one for convenience.
Reconciled balance	The matrix reconciles transactions within the stated coverage.	It does not prove the legality or reality of every transaction.

6.3 Independent review

The reviewer repeats calculations and relationships, checks duplicates, time zones, filters, versions, and correspondence with sources. The reviewer also tries to explain the discrepancy through another hypothesis: fee, batch, refund, date error, another channel, or missing document. A conclusion that works only by hiding a row cannot withstand review.

> **Closing**
> A strong financial report is not one that makes everything balance, but one that shows precisely what matches, what does not, why that might be, and what is still needed to decide.

Annex A. Reconciliation and request formats

A.1 Reconciliation matrix

Field	Required record	Control
Transaction	Identifier, date, amount, currency and parties.	Single unit of analysis.
Contract / order	Document, version and conditions.	Object and scope.
CFDI / XML	File, UUID, version and hash.	Not PDF alone.

Field	Required record	Control
Material performance	Delivery, performance and independent evidence.	Do not infer it from the folio.
Remittance / processor	Batch, channel, filters and coverage.	Do not mix periods.
Bank	Reference, instruction, settlement and channel.	Do not allocate by amount alone.
Accounting	Journal entry, period, currency and explanation.	Relationship with documents.
Status	Reconciled, partial, pending, duplicate or undetermined.	Do not force a match.

A.2 Request for financial records

Fictitious model for an authorized channel

```
Subject: EXP-DEMO-2026-010 · Transactions and associated records

Through the authorized channel, I request the supporting documents and records related to the references
included in the case file, covering [start and end with time zone].

Where available, include the instruction and settlement date/time, amount, currency, reference,
originator/beneficiary, channel, result, alerts, device, and authentication/enrollment events. State the
meaning of empty fields, filters, coverage, and retention.

Provide native format, PDF for review, data dictionary, process, and extraction date. In the response
body, state the algorithm and hash of each file. Preserve the delivery in EML with body, headers, and
attachments. Do not include credentials in that email.

Authorized representative · EXP-DEMO-2026-010
```

A.3 Unrecognized transaction matrix

Analysis worksheet

```
Transaction / reference: [identifier and source]
Account holder's allegation: [verbatim text and date]
Instruction and settlement: [events, time zone and channel]
Enrollment and factors: [additions, changes, deactivations]
Device and session: [available records]
System alerts and response: [rule and result]
Comparable transactions: [pattern and differences]
Communications: [notices and receipt]
Hypotheses A / B / C: [explanations]
Sources that distinguish them: [checks]
Technical result: [compatible, incompatible or inconclusive]
Applicable regime: [instrument, article, regulated entity and date]
Limits: [coverage and missing data]
```

Annex B. Comparative documentary framework and final review

Functional equivalence focuses on electronic documents, preservation, attribution, evaluation, and sector-specific records. Mexico combines CCom 89–94 and 1205, CFPC/CNPCF according to the transition, NOM-151, and CNBV; Peru separates IOFE, procedure, and SBS; Chile distinguishes signature and security; Argentina uses Law 25.506, CCyC, and BCRA; Colombia integrates Law 527 and CPACA;

Ecuador uses Law 67 and its payment regime; Spain combines eIDAS, LEC, and RD-ley 19/2018.[7891011121314151617181920212223]

Equivalence does not turn the rules into a single worldwide obligation. Cite function + instrument + article + regulated entity + version. If a source does not establish deadlines or paragraph numbers, mark them pending rather than inventing them. Financial and personal information must be handled with restricted access and data minimization.[24252627]

Final review	Acceptance question
Source	Are XML, bank, delivery, process and data dictionary available?
Coverage	Are the period, channels, accounts and filters documented?
Reconciliation	Does every relationship have an identity, not just an amount?
Material performance	Is the actual transaction separated from the document?
Authentication	Were enrollment, alerts and recovery reviewed?
Chronology	Are issuance, instruction, settlement and recording separated?
Conclusion	Is consent or liability attributed on the basis of a single signal?

[7]Mexico's Commercial Code, Articles 89–94 and 1205: neutrality, attribution, written form, original form, integrity, accessibility, and admissibility of data messages. Official compilation. Official online source

[8]National Code of Civil and Family Procedure, Articles 348–350. Compilation including the reform of 15-01-2026. Implementation is gradual and depends on official declarations. Official online source

[9]NOM-151-SCFI-2016, preservation and digitization of data messages, published 30-03-2017. Requirements for recordkeeping, integrity, accessibility, and electronic digital fingerprints. Official online source

[10]General provisions applicable to credit institutions, Articles 316 Bis, 316 Bis 1, and 316 Bis 10 to 17: supporting documents, encryption, access, incidents, operational incidents, logs, and reviews. Official online source

[11]Peru. IOFE Regulation, DS 052-2008-PCM, Articles 3 and 4: requirement and admissibility of digitally signed electronic documents. Official online source

[12]Peru. SBS 2286-2024: amendment to Article 20.3 on certain unrecognized transactions and liability, unless the user's liability is proven. Official online source

[13]Chile. Law 19.799 on electronic documents and electronic signatures, Articles 1–5: equivalence, written form, simple/advanced signatures, date, and probative value. Official online source

[14]Chile. Updated Compilation of Standards, Chapters 20-7, 20-8 and 20-10: outsourcing, operational incidents, information security and cybersecurity. Official online source

[15]Argentina. Civil and Commercial Code, Articles 318–319: correspondence by any means and assessment of the reliability of technical media and procedures. Official online source

[16]Argentina. BCRA Communication A 7783: digital transaction records available for at least 90 days and monitoring of security events. Official online source

[17]Colombia. Law 527 of 1999, Articles 5–13, 16–25 and 28: data messages, written form, original form, integrity, admissibility, preservation, dispatch, receipt and digital signature. Official online source

[18]Colombia. CPACA, Articles 57–58, 61 and 62: authenticity and integrity of administrative acts and electronic archives, acknowledgment of receipt and records of service failures. Official online source

[19]Ecuador. Law on Electronic Commerce, Electronic Signatures and Data Messages, Law 67, Articles 2, 6–8 and 10–16: equivalence, written form, original form, preservation, origin, dispatch, receipt and electronic signature. Official online source

[20]Ecuador. Resolution JPRM-2025-006-M, Official Register Supplement 104, 18-08-2025: operation, validity, clearing, settlement and availability of funds in payment systems. Official online source

[21]Regulation (EU) No 910/2014 eIDAS, Articles 25–26 and 46: non-discrimination of electronic signatures and documents based on their format, advanced signatures, and effects of qualified signatures. Official online source

[22]Spain. Civil Procedure Law, Articles 326 and 384: private documents, challenges, instruments for archiving, accessing or reproducing data, examination, custody, and sound judicial assessment. Official online source

[23]Spain. Royal Decree-Law 19/2018, Articles 45, 66 and 67: restitution for unauthorized transactions, risk management, and immediate notification of serious incidents. Official online source

[24]Colombia. Financial Superintendence. External Circular 033 of 2020, identified as an instruction on security and cybersecurity; its specific paragraphs must be confirmed before imposing specific obligations. Official online source

[25]Mexico. Federal Law on the Protection of Personal Data Held by Private Parties, text published 20-03-2025 and amended 14-11-2025. Articles 5–9, 18–20 and 31: principles, security, confidentiality, breaches and handling of data-subject rights requests. The current federal authority is the Secretariat for Anti-Corruption and Good Governance. Official online source

[26]Ecuador. Organic Law on the Protection of Personal Data, Official Register Supplement 459, 26-05-2021. Articles 10, 37–44: principles, security measures, protection by design, risks and incident handling. Official online source

[27]European Union. Regulation (EU) 2016/679, Articles 5, 25, 28 and 32–34: principles, protection by design, processors, security, and notification/communication of security breaches. Spain also requires review of the applicable national and sector-specific legislation. Official online source

Closing

The accounts may balance while the question remains open. Forensic analysis adds value when it shows what lies behind the document and what cannot be proven.