Master Data Governance Rules

Idea In Short

Start master data governance with one record type that causes recurring problems, such as supplier records, and assign three responsibilities: a data owner who sets standards, a steward who checks and maintains records and an approver who authorizes changes. Match checks to risk. A spelling correction can follow a simple route, while changes to payment details need independent verification through an established contact channel and approval by a reviewer who did not make the request. Document the exception route, retain a history of previous and new values and decide in advance which changes software may approve automatically. Track unresolved exceptions, requests returned for missing evidence and approval turnaround to see whether the process works.

Correcting a supplier's display name and changing its bank details touch the same business record, yet they call for different checks. Master data governance sets the rules for who can create, change and approve records that several departments share. It establishes responsibilities, definitions and checks for information about customers, suppliers and products. A supplier record is master data, which IBM describes as core data about key business entities that changes less often than the transactions referring to it.1 An invoice, by contrast, is a transaction linked to that record. Purchasing and finance need agreement about which supplier details to trust and who has the authority to alter them. Without that agreement, each department fixes what it sees in its own way. Purchasing corrects a name, finance edits a bank account, and the two versions of the supplier drift apart until an invoice lands on a record that nobody can vouch for.

Governance versus master data management

Governance determines authority and standards. Master data management does the practical work of maintaining, reconciling and distributing records under those rules. Data governance is a set of principles, policies and processes that guide how an organization makes decisions about data and who answers for it, from creation through disposal.2

Requiring independent approval before supplier payment details change is a governance decision. Checking the request, updating the approved record and sending the change to connected systems are management activities. Likewise, removing duplicates is a management task, while deciding which evidence takes precedence when records conflict is a governance decision. The dividing line is simple to apply: if the question is who decides or what standard applies, it belongs to governance, and if the question is how to carry out the decision, it belongs to management. Keeping the two apart stops a technician from quietly making a policy choice while cleaning up data.

Before adopting artificial intelligence [AI] workflow automation in an enterprise resource planning [ERP] system, such as the one the vendor advertises as Priority AI ERP, a business needs to define which changes can proceed automatically and which require human approval. Those decisions guide how the software controls are set up. A tool can enforce a rule only after someone has written it down, so governance comes first and the software follows. A team that sets up the software first ends up encoding its existing habits, and nobody can later explain why a given change was approved.

Who owns, maintains and approves records

Responsibility for a record belongs with the people who understand how the business uses it. Information technology [IT] maintains the systems underneath, so it plays a supporting role and does not automatically own every record. A practical starting arrangement separates three functions:

- Data owner: sets standards, accepts accountability and resolves disputed decisions within policy
- Data steward: checks requests, maintains records and investigates quality issues
- Approver: authorizes specified changes after reviewing the required evidence

These are responsibilities, not necessarily separate job titles. In a mid-sized company, for instance, the head of purchasing might own supplier records, accounts payable staff might act as stewards and the finance controller might approve changes to payment details. Someone in a small organization might hold several of them, with independent approval retained for higher-risk changes. That independence applies an old control principle. The National Institute of Standards and Technology [NIST] defines separation of duty as the idea that no user should have enough privileges to misuse the system alone.3 Document the

limits of each person's authority, including which corrections a steward can make directly. Name deputies so that requests follow the agreed process during absences. Otherwise, a request that waits for an absent approver finds an informal shortcut, and the shortcut becomes the real process.

A supplier-record change, from request to approval

Consider a hypothetical supplier that asks a business to correct a spelling error and replace its payment details. One request can cover both changes, but the checks differ by field. The spelling change affects how the supplier appears on documents. The payment change redirects money, so it carries the greater risk. A wrong name is an inconvenience. A wrong account sends cash to a stranger. The sequence below follows the request from receipt to the updated record. It works for any shared record whose fields carry different levels of risk.

Capture and check the request

First, record the supplier's unique identifier, the affected fields, the proposed values, the requester and the supporting evidence. Match the request to the existing record, which avoids creating a duplicate under the corrected name. Keep proposed values separate from approved ones while checks are underway. Nobody should see an unverified bank account in the live record. The steward then checks that the request is complete and that the supplier identifier matches. Format validation shows whether a bank-account entry follows an expected structure. It cannot show who owns the account, and that takes independent verification. Use an established supplier contact route, not a telephone number supplied in the change request. The FBI's Internet Crime Complaint Center gives the same advice for business email compromise: confirm requests for changes in account information through a secondary channel, a scam category it linked to about $55.5 billion in exposed losses between October 2013 and December 2023.4

Apply the approval rule for each field

Next, apply the approval rule for each field. A spelling correction that leaves the supplier's legal identity unchanged could follow a simpler route. A change of legal entity needs additional checks, because it changes who the business contracts with and pays. Payment details should go to an authorized reviewer who is independent of the requester. Record what was checked and the reasons for accepting or rejecting the proposal. Write the reason

in plain words, such as the evidence reviewed and the contact route used to confirm it. That record lets a later reviewer test the decision against the policy instead of relying on memory.

Resolve exceptions and record the outcome

If evidence conflicts or verification fails, keep the proposal pending and assign the exception to a named person. Flag affected payments for review and specify the information needed to resolve the exception. Disagreements between departments go to the data owner, who decides in line with the documented policy. Once approved, update the authoritative record and confirm that the relevant purchasing and payment systems receive the change. Retain a history showing the previous and new values, the requester, the reviewer and the decision time. This history answers the questions that come up months later, such as why a payment went to a new account on a given date. Auditors, colleagues and the supplier itself can then see the same facts.

Start with one record type and review the results

Choose a record type that causes recurring problems, such as a supplier file with frequent duplicate entries or disputed bank details. A narrow scope lets the team test the roles, the checks and the exception route on a volume it can manage. Success on one record type also gives the team a working example to show other departments. Define its essential fields, identify the approved source for each and assign authority to request, check and approve changes. This creates a manageable starting point before you extend governance to other records. Document the exception route alongside the normal process, so staff know where to take missing evidence or disputed information. Staff should never have to guess whom to ask. Review a few clearly defined measures:

- Unresolved exceptions, counted at a fixed review point
- Requests returned for missing evidence
- Approval turnaround, measured from receipt of a complete request to the recorded decision, with incomplete requests tracked separately so their delays stay visible

Review the request form when evidence keeps going missing, and clarify authority where disputes stay open. A workable governance process lets staff trace a change from request to resolution and identify who is responsible at every stage.

- 1What is master data management? | IBM
- 2Data governance
- 3Separation of duty (SOD) - Glossary | CSRC
- 4Business email compromise: The $55 billion scam

Summary

Master data governance answers one question for every shared record: who may create, change and approve it, and on what evidence. Governance sets authority and standards, master data management carries out the maintenance under those rules, and software enforces only what people have first written down. A supplier-record change shows the principle in practice, because a name correction and a bank-detail replacement share a record but not a risk. Starting with one record type, naming owners, stewards and approvers and reviewing a few measures lets a business trace any change from request to resolution and identify who answered for each stage.