

# Master Data Governance: Order and Control for Procurement Data

Master data governance refers to the sum of policies, roles, processes and controls with which companies ensure the quality, consistency and use of their master data. In industrial procurement, this particularly concerns supplier, material, item and contract master data, on which almost all procurement processes are built. Effective governance prevents duplicates, incorrect allocations and process friction losses that would otherwise impact orders, goods receipt and the invoice approval workflow all the way into the supply chain.

## Key facts

- Master data governance governs responsibilities, quality standards and change processes for master data such as supplier, material and contract data.
- Typical components in practice are a data owner model, defined data field standards as well as release and quality workflows.
- Measurable metrics include data quality rates, duplicate rates and the completeness of central fields such as supplier or material classification.
- Good master data directly impacts operational metrics such as On-Time Delivery (OTD) and On-Time In Full (OTIF) because sourcing and materials planning rely on reliable data.
- Typical benchmarks from practice: completeness of critical fields above 95%, duplicate rate below 2%, processing times for new records often under 48 hours.
- Governance is an ongoing process, not a one-off project; it should be anchored in the category roadmap and in vendor onboarding.

## Definition: Master data governance

Master data governance is the organisational and process framework for steering company-wide master data quality. It defines who may create, change and release which data, which standards apply and how data errors are prevented or corrected. In procurement, it thus forms the foundation for sourcing, supplier management and operational processing.

## Distinction from data quality and data management

Data quality is the goal, data management the operational implementation – governance provides the structural perspective with policies, roles and controls. Master data differs from movement or transaction data in that it remains valid over long periods: supplier addresses, material numbers, classifications or contract terms. Precisely this longevity makes errors expensive, because an incorrect entry persists across hundreds of orders and invoices. Governance therefore ensures that quality rules are adhered to not just once, but permanently.

## Relevance for technical procurement

Technical buyers work with highly complex material master data: drawing numbers, material

designations, standards, bill-of-materials positions. Without governance, parallel material numbers arise for identical parts, which leads to double purchasing, distorted spend analytics and unnecessary requalification efforts with suppliers. Consistent supplier master data is also a prerequisite for supplier discovery and evaluation in the supplier portfolio. Governance therefore indirectly determines procurement costs, ability to deliver and auditability.

## Structure of master data governance in procurement

A robust governance combines a clear responsibility model with operationalised processes for creation, change and quality checking. It should be embedded in existing procurement structures and not run as an isolated data function alongside the business.

### Role model and responsibilities

A three-level model has proven effective: data owner (responsible in terms of content, typically the category manager), data steward (operationally responsible for maintenance and quality control) and data user (buyers, planners, specialist departments). Allocation should sensibly follow a RACI scheme, as is also common for roles in procurement (RACI). It is important to clearly separate creation and release: whoever creates a supplier should not release them on their own authority – especially in vendor onboarding with credit checks, compliance screening and bank detail verification, a four-eyes structure is often mandatory.

- Data owner: content responsibility for the data domain, e.g. suppliers or materials
- Data steward: operational maintenance, quality control, duplicate clarification
- Data user: read access, feedback on data errors via a defined channel

### Data field standards and maintenance processes

Governance is concretised in binding field definitions: which mandatory fields must be filled in a material master, which classification systems are used, how are descriptions worded? In practice, naming conventions, controlled value lists and integration with classification standards have proven effective. Changes go through documented change requests with review steps; for critical changes such as bank details or deviating delivery addresses, additional controls are required, as these constitute a classic gateway for fraud.

### Anchoring in procurement processes

Master data governance only has an effect if it is integrated into the process chain: in vendor onboarding, supplier master data is created in a structured and validated way; in tendering, the data pool feeds the award timetable; and in series ramp-up (SOP), material and drawing data must be consistent between customer and supplier. In transfer of work or outsourcing transitions too, the migration and qualification of master data is part of the handover packages.

## Key KPIs of master data governance

Data quality can only be managed if it is made measurable. A small number of clearly defined metrics that are evaluated regularly – typically monthly or quarterly – and reported to management have proven effective.

### Quality and completeness metrics

The completeness of critical fields (e.g. classification, contact person, payment terms) is measured as a

percentage of the total volume; in practice, values above 95% are considered a good benchmark. The duplicate rate shows how many unnecessary parallel records exist – values below 2% are common as a target. In addition, the error rate per new record and the average turnaround time for change requests are measured, as slow processes undermine acceptance of governance.

### **Impact metrics at process level**

Beyond pure data metrics, it is worth looking at effects: how many invoices in the invoice approval workflow fail due to incorrect master data? What proportion of goods receipts are manually corrected? And to what extent do correct material and supplier data support the meaningfulness of metrics such as On-Time Delivery (OTD) or On-Time In Full (OTIF)? Incorrect shipping plant or address data, for example, distorts the delivery deviation analysis and leads to unnecessary delivery chasing even though the delivery was en route correctly.

## **Methods and approach for introduction**

Introduction works best as a step-by-step programme with clear prioritisation. A big bang across all data domains frequently fails in practice due to resources and acceptance.

### **Inventory and prioritisation**

The starting point is a data inventory: how many material and supplier masters exist, what are the duplicate and error rates, which fields are critical for processes and reporting? From this a prioritisation is derived – typically first the domains with the greatest process damage, for example material master data where double purchasing is high, or supplier master data with compliance relevance. The results ideally feed into the category roadmap so that data cleansing and strategic procurement planning go hand in hand.

### **Cleansing and deduplication**

Before rules are introduced, the existing data is cleansed: duplicates are identified and merged, incomplete records are completed, outdated entries are archived. For material master data, this often includes coordination with engineering and production, since drawing and material data can only be corrected with technical review. The cleansing produces typical error patterns that are then automatically intercepted by rules – for example mandatory field checks during creation or warnings for similar descriptions.

### **Technical implementation**

Governance needs technical backing: mandatory field logic in the ERP, workflow approvals, duplicate checks during creation and ideally a master data management system as the leading system. What is decisive is that rules are enforced in the system and not merely documented. At the same time, the following applies: software does not replace responsibility – without named stewards and established bodies, every solution remains a paper tiger.

## **Risks and controls**

Weak master data governance carries operational, financial and legal risks. Control is exercised through defined review processes and regular audits.

## Typical risks

Incorrect bank details in the supplier master open the door for fraudsters to divert payments – controls here must be designed with particular care. Duplicates cause double purchasing and distort the supplier portfolio; incorrect material data leads to wrong orders and quality problems up to a line stop if the wrong part number is ordered or delivered. Incomplete compliance and certificate data can lead to breaches of documentation obligations – here case-by-case review by the legal or compliance department is recommended.

## Control instruments

Proven controls are: the four-eyes principle for critical changes, regular duplicate and completeness audits, controlled access rights (who may change which fields) and a documented complaint and correction process for data errors. For sensitive fields such as bank details, reverification via a second, independent channel – typically by telephone with a known, verified contact person – is standard practice.

## Current developments: digitalisation and supplier networks

Master data governance is changing through integration with suppliers and the increasing automation of data maintenance. Data capture is increasingly shifting to the source.

### Self-disclosure and supplier networks

Via a supplier network, suppliers enter their master data themselves – addresses, certificates, contact details, capacities – and the buyer reviews and releases it. This significantly reduces maintenance effort and error rates, but shifts control to review processes. Supplier discovery works in a similar way: its usefulness depends directly on structured and classified supplier and material master data being available, otherwise search results and enrichments can hardly be evaluated.

### Automation and AI-supported classification

Algorithms increasingly support material classification, duplicate detection and enrichment from external sources. This accelerates maintenance but requires clear governance rules: who bears responsibility for AI suggestions, how are releases documented, how is accuracy verified? The trend is towards a hybrid model – machine suggestions, human release for critical fields, automatic release for uncritical standard changes.

### Regulatory drivers

Increasing reporting obligations along the supply chain – for example on supply chain and sustainability requirements – are expanding the concept of master data: certificates, origin data, tier-n transparency and suppliers' sustainability indicators are becoming mandatory fields. Product compliance data and material information are also gaining relevance. Governance must define these fields from the outset so that they do not have to be added retrospectively with gaps. The concrete implementation of legal obligations should always be reviewed legally on a case-by-case basis.

## Typical metrics

### Completeness of critical fields: > 95%

Practical benchmark; weighted differently depending on domain (supplier/material)

**Duplicate rate: < 2%**

Proportion of unnecessary parallel records in the total volume

**Turnaround time for change requests: < 48 h**

frequently targeted benchmark for standard changes

**Error rate for new records: < 5%**

Proportion of new records requiring subsequent correction

## Practical example

A medium-sized mechanical engineering company with around 200 employees discovered during a spend analysis that a frequently used standard cutting part was maintained under four different material numbers – each with different suppliers and prices. At the same time, incomplete supplier master data regularly delayed the invoice approval workflow chain because payment terms or contact persons were missing. The company established a lean master data governance: the category manager acted as data owner, two procurement staff took on the steward role. Within nine months, the material masters were consolidated, mandatory field rules were enforced in the ERP and vendor onboarding was digitised via a structured self-disclosure process.

- Duplicate cleansing of material master data with engineering and production
- Introduction of a RACI model for creation, change and release
- Four-eyes control for critical supplier changes such as bank details
- Quarterly quality reporting with completeness and duplicate metrics

## Conclusion

In industrial procurement, master data governance is not an end in itself but the foundation for reliable sourcing decisions, smooth operational processes and meaningful reporting. It only works when responsibilities are clearly named, rules are enforced in the system and quality is measured regularly. The effort pays off twice: it reduces direct costs through fewer duplicates and incorrect postings and indirectly improves metrics such as OTIF and OTD because these are built on reliable data. Companies that prioritise governance step by step and integrate it into existing processes such as vendor onboarding and category planning achieve viable results faster in practice than with a comprehensive large-scale project.

## Frequently asked questions

### What does master data governance mean in procurement?

Master data governance encompasses the policies, roles and processes with which companies control the quality of their supplier, material and contract master data. It defines who creates, changes and releases data, which field standards apply and how errors are prevented. In procurement, it forms the foundation for sourcing, materials planning and invoice processing.

### What roles exist in master data governance?

A three-level model is typical: the data owner is responsible in terms of content (often the category manager), the data steward maintains the data operationally and monitors quality, and data users work with the data in day-to-day business. Allocation is usually done via a RACI scheme. It is important to separate creation and release, especially for sensitive changes.

## **How is master data quality measured?**

Common metrics are the completeness of critical fields (benchmark above 95%), the duplicate rate (target often below 2%), the error rate for new records and the turnaround time for change requests. In addition, impact metrics are considered, such as the number of invoices that fail in the approval workflow due to incorrect master data. The metrics should be collected regularly and with consistent definitions.

## **Why is master data important for OTIF and OTD?**

Delivery metrics such as On-Time In Full (OTIF) and On-Time Delivery (OTD) depend on correct shipping plant, address and material data. Incorrect master data leads to wrong deliveries, incorrect delivery locations or parts that cannot be supplied – and thus distorts the metric itself. In addition, delivery deviation analysis and delivery chasing depend on the system inventory matching reality.

## **How do you start a master data governance project in procurement?**

A step-by-step approach has proven effective: an inventory with duplicate and completeness analysis, prioritisation by process damage, then cleansing of the most critical domains. In parallel, roles and field standards are defined and enforced in the ERP. Anchoring in existing processes such as vendor onboarding and the category roadmap ensures sustainability.

## **What risks arise from poor master data?**

Incorrect bank details can enable payment diversion, duplicates cause double purchasing, and incorrect material data can in the worst case lead to wrong deliveries up to a line stop. In addition, metrics such as spend analytics and supplier ratings lose their meaningfulness. Regular audits, access rights and four-eyes principles for critical changes are the most important controls.