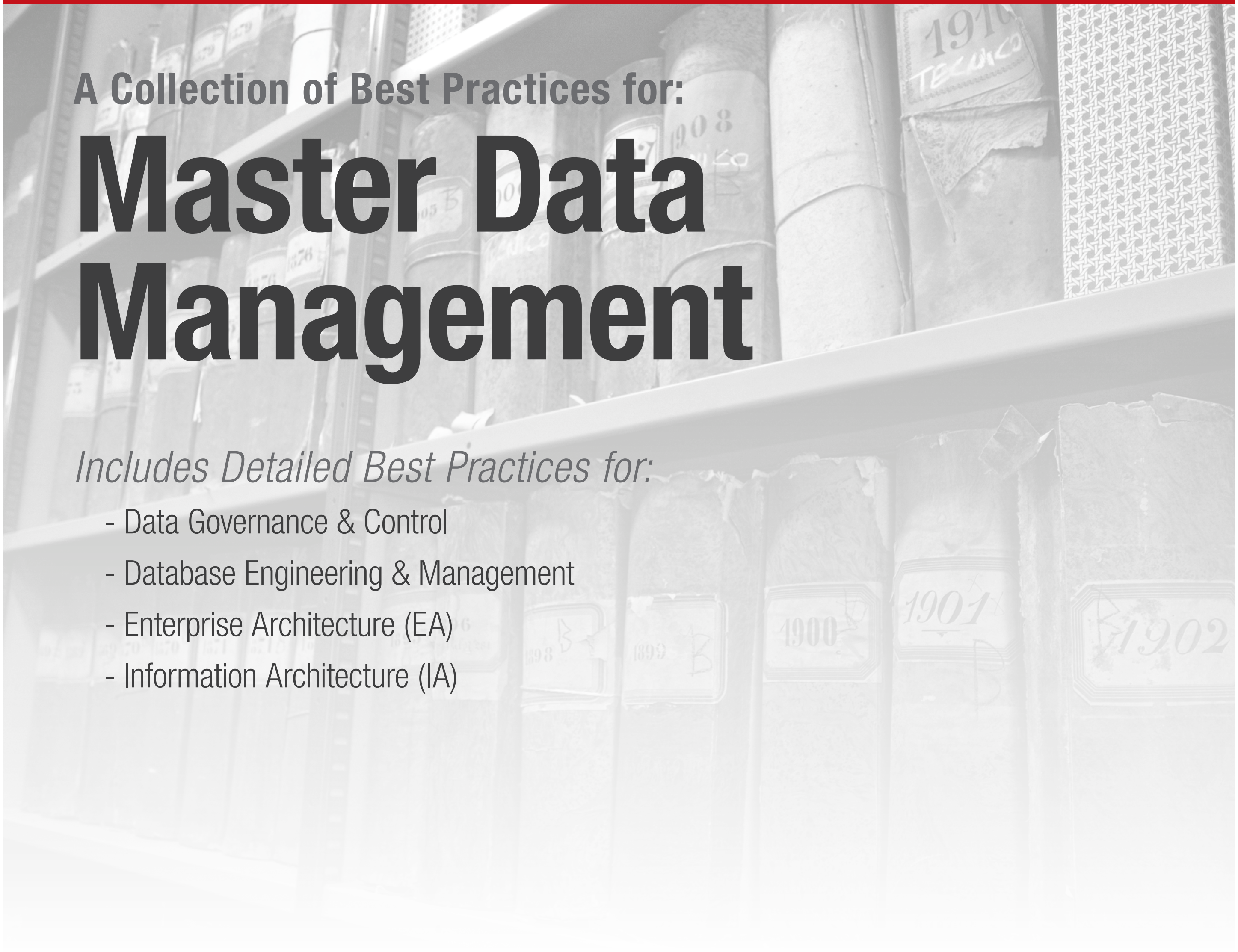
BEST PRACTICES



A Collection of Best Practices for:

Master Data Management

Includes Detailed Best Practices for:

- Data Governance & Control
- Database Engineering & Management
- Enterprise Architecture (EA)
- Information Architecture (IA)

opsdog©

Table of Contents

Master Data Management Best Practices

Master Data Management Best Practices

This content may not be copied, distributed, republished, uploaded, posted or transmitted in any way without the prior written consent of OpsDog, Inc.

Data Governance & Control

Master Data Management

- **Data Governance & Control**
- Database Engineering & Management
- Enterprise Architecture (EA)
- Information Architecture (IA)

The Data Governance and Control function is responsible for developing company-wide policies regarding data use and setting standards for data quality and security. They work with business units to maintain analytical and reporting capabilities by enforcing the quality, consistency and cleanliness of the data that they produce and manage. They may also coordinate across organizational groups communicate and enforce data naming conventions, recordation methods, and metadata inputs to foster cross-organizational data sharing and comparability.

Data Governance & Control

Master Data Management Best Practices

Best Practice 1-A

Periodically Train Employees on Data Governance Policies and Data Literacy to Ensure Compliance

Develop and clearly define data governance policies and processes, especially those governing the storage of internal and external data, so as to ensure employee understanding and compliance. Use periodic training programs, meetings and various reference materials (physical or online based) to increase end user data literacy and ensure they are kept up-to-date on any policy or procedural updates.

Typical Practice (the Status Quo): Train employees on complying with company data governance policies upon being hired to quickly bring them up to speed with what is expected. Provide employees easy access to physical (manuals, brochures, etc.) and online resources for them to refer back to. It is the responsibility of the employees to understand and comply with company data governance policies.

Benefits of this Best Practice: To ensure company-wide standardization concerning data governance (the overall management of the availability, usability, integrity and security of a company's data), employees must not only understand the data governance policies and processes, but they also need to know how to efficiently comply with those policies. In this regard, the Data Governance & Control Group must make sure that all policies are clearly defined while also striving to increase the data literacy of the company's end-users (the employees). To do so, training programs, meetings and reference materials (both physical and online resources) should focus on teaching employees how to distinguish good data from bad data in the context of their decision making environment and role in the organization, how to use data analysis tools, process improvement techniques, etc.

Related KPIs: Training Hours per Employee, Unit Cost: Employee Training, Percentage of CRM Fields with Missing Data, Database Uptime, Data Field Standardization Rate, Data Record Error Rate

Best Practice 1-B

Perform Periodic Data-Securing Tool Updates to Efficiently Protect Data Integrity

Periodically update data-securing measures and all corresponding tools (anti-malware software, firewalls, encryptions, audit logs, passwords, etc.) to ensure efficiency in guarding against unapproved use or the corruption of data. Use meetings to train and encourage employees to report any suspicious activity or incident. Otherwise, use standardized checklists to keep on top of security tool updates.

Typical Practice (the Status Quo): Purchase the most current version of various data-securing tools and use them for as long as possible. Continuous updates can cost the company a lot of money, and have little to no direct results. Furthermore, it is the responsibility of the employees themselves to ensure that the data they store and use are kept safe by not performing unsafe data practices (clicking on links from unknown emails, going to websites that are considered unsafe, etc.).

Benefits of this Best Practice: All data (especially data deemed to be sensitive such as personally identifiable information) is suspect to potential unauthorized modification or destruction. Note that certain kinds of sensitive data (financial data, health data or