LOLA Linked Organisation of Local Authority ICT Societies

Data insight and analytics

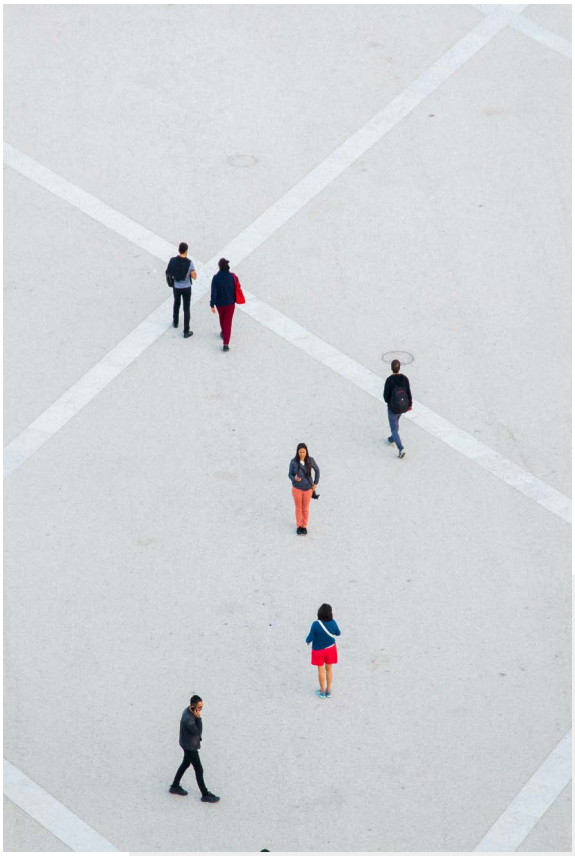
Guide | June 2022

Introduction

Data management is in the spotlight more than ever. Recent events have accelerated interest in sourcing relevant data, in creating solutions to manage information, and in generating intelligence to inform policy and practical interventions. The amount of data in and around our organisations is only increasing. And, with it, also is the need to use it effectively and efficiently. The better we are at using data well, the greater the benefits we can derive from it. The result can translate into lower costs, greater efficiency, competitive advantages, and better outcomes. It is therefore important to immerse ourselves in the application and opportunities of data management.

Data management is about maintaining, updating, managing, and securing data. Data files are checked for accuracy and adjusted if necessary. Existing files are enriched with new and additional data from external sources. Thanks to links with external files, keeping data up to date can increasingly be automated. Data management aims to ensure that the available data is complete, reliable, and available on time for applications that use that data. This may be dependent on business software or other IT systems. Based on good and complete data, you can – after analysing it – optimise the execution of business processes and help you make the right decisions. The addition of the term 'enterprise' before the term data management (EDM) emphasises that this concerns the management of data, not just across whole organisations but also across whole ecosystems of multiple organisations.

We can also work with data governance. Data governance is the exercise of authority, control, and shared decision-making (planning, monitoring, and enforcement) over the management of data assets and adherence to common standards. Data governance represents an inherent separation of duty between oversight and execution.



Purpose of this paper

This paper aims to provide a simple guide to harnessing data insight and analytics within a local, place-based context. It has been developed using the knowledge and experience of practitioners from LOLA's network of eight professional associations. It sets out seven strategic principles, an operating model for roles and responsibilities, the benefits of Master Data Management, and five areas for adherence to standards.

Seven strategic principles

1. Promote the consistent use of data to improve community engagement.

By adopting this principle, community engagement will be more effortless and responsive to user needs. Data can help the city, town or region better understand the needs of its users and generate insights to predict future behaviours. Greater access to data will enable more effective decision-making and local service providers to respond to information requests and deliver services in a more nuanced, effective, and timely manner.

2. Encourage data-powered innovation to turn data into actionable insights.

Public service decisions are increasingly dependent upon insights. By encouraging data-powered innovations, the government will be better positioned to understand citizen behaviours, its operating environment, and employee engagement. Ultimately, actionable insights will help the local authorities to deliver improved services.

3. Recognise data as a strategic asset and establish fit-for-purpose.

This principle recognises that data is a strategic asset for the government because it can help the decision-making process and give the government a better insight into its processes. By adopting this principle, the government will manage data as carefully as any other valuable asset. Local and national public sector data has played a key role in managing the Covid crisis. Therefore, the accessibility and usability of this type of data need to be placed at the forefront of local and national policy agendas because it can also play an immense role in our day-to-day work and policies.

4. Make data visible and accessible, recognizing that data is curated by the local government authority

This principle echoes the local governments' need to be a data-driven organisation. To achieve this, data must be made visible and accessible across the entire organisation, in line with appropriate privacy and security policies. The local government should remove data silos and involve all departments in managing data. This principle also emphasises that local government has a role in curating data to empower citizens and employees.

5. Maintain data quality, data integrity, and one source of truth.

With the increasing sophistication of technology, the employees, processes, and systems will collect vast amounts of data from a growing number of functional areas. By adopting this principle, the local government will improve the quality of data that it owns. This increases its employees' and customers' trust in data and enables the local government to make more accurate data-driven decisions.

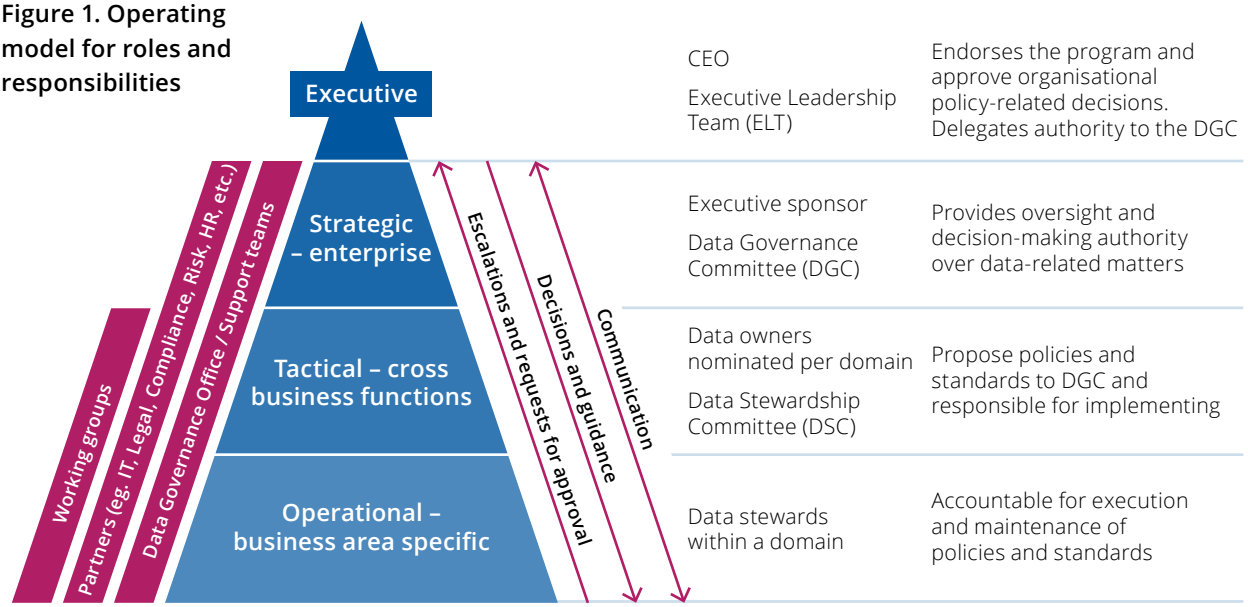
6. Embed privacy and security controls across the organisation.

Laws and regulations require the local government to safeguard the privacy of data. This principle calls for the local government to adopt strong security measures to safeguard data privacy.

7. Enhance cross-sectoral data sharing

The Covid crisis made local governments rapidly acquire and share data with a range of cross-sector organisations, in particular health care services, the central government, and the third sectors, to manage and coordinate a local response to the pandemic. We need to maintain this cross-sectoral

Figure 1. Operating model for roles and responsibilities



data sharing for different policy issues. Therefore, we will need to focus more than ever on consolidating data sharing protocols across the public sector, developing data sharing protocols with the third sector, and investing in national data ecosystems.

Operating model for roles and responsibilities

The Data Governance Committee

The Data Governance Committee (DGC) is the highest tier data governance organisation in an enterprise, responsible for oversight, support, and sponsorship of data governance activities. The ELT will delegate certain authorities and responsibilities to the DGC.

The Data Owners

Data Owners are business Data Stewards, who have approval authority for decisions about data within their domain. Affiliation to their business area becomes secondary and they represent an enterprise view for data-related matters.

The Data Stewardship Committee

The Data Stewardship Committee (DSC) is staff from the business who represent the voice of the City and the community for input into policies, procedures, and solutions. They may make recommendations or escalate issues for decision by the DGC. The DSC may break out into teams or working groups that address specific data issues or decisions.

The Data Stewards

Data Stewards manage data assets on behalf of others and in the best interests of the organisation. They are business professionals, most often recognised subject matter experts, accountable for a subset of data. They work with stakeholders to define and control data.

The Data Governance Office

The Data Governance Office is the hub for enterprise-wide data governance and data management practices. They support the DGC, DSC, and Data Communities.

Top six benefits of Master Data Management

1. Accurate, complete, and consistent citizen data across departments and agencies

Many agencies struggle with having separate departments operate in data silos. A complete view of citizen data for streamlined processing and decision-making is key for a 21st-century government. MDM enables support for multi-agency (or multi-departmental) working and care coordination, with tracking and alerts for significant information.

2. A holistic view of service consumption for more informed decisions

Understand how citizens interact and engage with the government across multiple departments or agencies. MDM enables agencies to be more proactive and timely in their service delivery and efficiency, and in their reporting, analytics and monitoring/tracking.

3. Streamlined services delivered at a lower cost

MDM enables data stewards to do their job quickly and efficiently. It improves user experience, and uptake in citizen experience (in self-service models), making more services available online. MDM allows agencies to eliminate manual, burdensome data entry and improve operational efficiency and strategic planning, ultimately improving data quality while reducing cost and resources.

4. A common policy point for the front office, back office, and citizen self-service

A single, 360-degree view of enterprise data provides ease of use and data consistency across all departments and channels. Data is maintained from a single point of view, communicating from this "golden record" back out to the sources it's ingested from, so everyone is always on the same page. If the back end has all the correct and matched data, citizens can use the portal to get to what they need on their own, which is more efficient and less costly.

5. A common data backbone for digital transformation

MDM integrates CRM with back-office systems to provide services from a single point of view, with sophisticated search capabilities. It allows users to handle more citizen inquiries the first time, reducing avoidable, unnecessary follow-up contact. Consent and privacy are managed centrally, reducing security risks and improving compliance.

6. Better outcomes – and a better experience – for the citizen

MDM allows for more timely and appropriate interactions to provide better outcomes, both internally and externally. It makes processes faster, more efficient, and enables evolution to more self-service channels. Data quality and consistency are improved across all systems.

Standards

Adherence to common standards and data sharing protocols represents a key area of challenge, yet one that is essential to effectively harnessing data and delivering meaningful services to residents in a local, place-based context.

Standards for governance	
Security Management Framework	An organisation must establish, implement and maintain a security management framework that is proportionate to its size, resources, and risk posture.
Security Risk Management	An organisation must utilise a risk management framework to manage security risks.
Security Policies and Procedures	An organisation must establish, implement and maintain security policies and procedures proportionate to their size, resources, and risk posture.
Information Access	An organisation must establish, implement and maintain an access management regime for access to public sector data.
Security Obligations	An organisation must define, document, communicate and regularly review the security obligations of all persons with access to public sector data.
Security Training and Awareness	An organisation must ensure all persons with access to public sector data undertake security training and awareness.
Security Incident Management	An organisation must establish, implement and maintain a security incident management regime that is proportionate to its size, resources, and risk posture.
Business Continuity Management	An organisation must establish, implement and maintain a business continuity management program that addresses the security of public sector data.
Contracted Service Providers	An organisation must ensure that contracted service providers with access to public sector data, do not do an act or engage in a practice that contravenes the national and international regulations on cyber and information security.
Government Services	As an organisation that provides a government service to a State Agency, we must comply with the national and international regulations on cyber and information security. in respect to public sector data that is collected, held, used, managed, disclosed, or transferred.
Security Plans	An organisation must establish, implement and maintain a protective data security plan to manage their security risks.
Compliance	Local Government Agencies are exempt from reporting compliance to the Commissioner for Privacy and Data Protection.

Standards for information security

Information Value	An organisation must conduct an information assessment considering the potential compromise to the confidentiality, integrity, and availability of public sector data.
Information Management	An organisation must establish, implement, and maintain information security controls in its information management framework.
Information Sharing	An organisation must ensure that security controls are applied when sharing public sector data.

Standards for personnel security

Personnel Lifecycle	An organisation must establish, implement, and maintain personnel security controls in its personnel management regime.

Standards for ICT security

Information Communications Technology Lifecycle	An organisation must establish, implement and maintain Information Communications Technology (ICT) security controls in their ICT management regime.

Standards for physical security

Physical Lifecycle	An organisation must establish, implement and maintain physical security controls in its physical management regime.

About this guide

Editor

Milenco Van Quaethem
(Project Manager, V-ict-or)

Produced in association with

ALGIM, New Zealand ..... www.algim.org.nz
GMIS, USA ..... www.gmis.org
KommITS, Sweden ..... www.kommits.se
MAV Technology, Australia ..... www.mavdigital.com
MISA/ASIM, Canada ..... www.misa-asim.ca
Socitm, UK ..... www.socitm.net
VIAG, Netherlands ..... www.viag.nl
V-ict-or, Flanders ..... www.v-ict-or.be

Get in touch

www.lola-ict.org
info@lola-ict.org
+32 93 952 028

Gentstraat 9,
9250 Waasmunster,
Belgium

LOLA Linked Organisation of Local Authority ICT Societies