TECHNICAL SPECIFICATION

ISO/IEC TS 38505-3

First edition
2021-12

Information technology — Governance of data —

Part 3: Guidelines for data classification

Technologies de l'information — Gouvernance des technologies de l'information —

Reference number
ISO/IEC TS 38505-3:2021(E)

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see https://patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 40, *IT Service Management and IT Governance*.

A list of all parts in the ISO/IEC 38505 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

Introduction

This document complements the existing International Standards on IT governance (ISO/IEC 38500) and data governance (ISO/IEC 38505-1). It is designed to provide practical guidance for organizations including governing bodies and management to allow them to:

— maintain an oversight of their data portfolio,

— understand the business context, value, sensitivity and risk associated with the data, and

— apply mechanisms that are both proportionate and appropriate, ensuring that data is protected, and is only used for intended purposes consistent with the organization's obligations.

Information technology — Governance of data —

Part 3:
Guidelines for data classification

1 Scope

This document provides essential guidance for members of governing bodies of organizations and management on the use of data classification as a means to support the organization's overall data governance policy and associated systems. It sets out important factors to be considered in developing and deploying a data classification system.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at https://www.electropedia.org/

3.1
big data
extensive datasets, primarily in the data characteristics of volume, variety, velocity and/or variability, that require scalable technology for efficient storage, manipulation, management and analysis

Note 1 to entry: Big data is commonly used in many different ways, for example as the name of the scalable technology used to handle big data extensive datasets.

[SOURCE: ISO/IEC 20546:2019, 3.1.2, modified.]

3.2
customer data
data held on file about customers

Note 1 to entry: This comprises the information customers provide while interacting with the organization via their website, mobile applications, surveys, social media, marketing campaigns and other online and offline avenues.

3.3
data controller
person or organization who determines the purposes for which and the manner in which any data are to be processed, stored and used

[SOURCE: ISO 10667-1:2020, 3.10, modified.]

3.4
data processor
person [other than an employee of the *data controller* (3.3)] or organization that processes the data on behalf of the data controller.

[SOURCE: ISO 10667-1:2020, 3.11, modified.]

3.5
data quality owner
senior level employee accountable for the quality of one or more datasets

3.6
data sensitivity
property of data that reflects the potential harm of unauthorized disclosure

Note 1 to entry: The potential harm is to an individual or organization.

Note 2 to entry: Different levels of data protection can be used to account for varying levels of data sensitivity.

Note 3 to entry: Data sensitivity can be applied to specific categories of data such as healthcare, finance, *personal data* (3.12).

3.7
data sharing
access to or processing of the same data by more than one authorized entity

3.8
data stakeholder
natural or legal person that can affect, be affected by, or perceive themselves to be affected by a decision or activity related to the processing of data

3.9
data steward
role within an organization responsible for ensuring that data-related work is performed according to policies and practices as established through data governance

Note 1 to entry: Typically, data stewards are responsible for business controls, data content and meta-data management related to a set of data assets, utilizing an organization's data governance processes to ensure fitness of data elements, both the content and metadata.

[SOURCE: ISO/TR 14872:2019, 3.5, modified.]

3.10
data taxonomy
scheme for organizing data based upon relationships and common characteristics

Note 1 to entry: A data taxonomy can include data categorization and data classification; it represents a convenient way to organize data.

3.11
organizational data
class of data objects under the control, by legal, contractual or other reasons, of an organization.

Note 1 to entry: Organizational data are all business information and data that are accessed, collected, used, processed, stored, shared, distributed, transferred, disclosed, destroyed or disposed of by any of the business units. Organization data can include, for example, financial records, business strategy documents, governing body and governance papers, staff information (employees, contractors, consultants), business analysis and intelligence, and executive information.

Note 2 to entry: Organizational protected data, or OPD, is organizational data for which protection is required based on the policies established by the governance of data process.

Note 3 to entry: Organizations have policies that govern the data under their control. ISO/IEC 38505-1 identifies and examines higher level governance concerns regarding the use of data which is relevant from the perspective of governance of data.

Note 4 to entry: Organizational data can contain OPD and PII.

[SOURCE: ISO/IEC 19944-1:2020, 3.4.2, modified.]

3.12
personally identifiable information
PII
personal data
any information that (a) can be used to establish a link between the information and the natural person to whom such information relates, or (b) is or can be directly or indirectly linked to a natural person.

Note 1 to entry: The "natural person" in the definition is the *PII principal* (3.13). To determine whether a PII principal is identifiable, account should be taken of all the means which can reasonably be used by the privacy stakeholder holding the data, or by any other party, to establish the link between the set of PII and the natural person.

[SOURCE: ISO/IEC 29100:2011/Amd1:2018, 2.9, modified.]

3.13
PII principal
natural person to whom the *personally identifiable information (PII)* (3.12) relates

Note 1 to entry: Depending on the jurisdiction and the particular PII protection and privacy legislation, the synonym "data subject" can also be used instead of the term "PII principal".

[SOURCE: ISO/IEC 29100:2011, 2.11]

3.14
semi-structured data
aggregate datatype whose components' datatypes and their labels are not pre-determined

Note 1 to entry: Semi-structured data are forms of *structured data* (3.15) that do not follow the formal structure of data models related to relational databases or other forms of databases.

Note 2 to entry: Examples of semi-structured data include the data that contain HTML tags or other markers to separate semantic elements and to represent hierarchies of records and fields within the data.

[SOURCE: ISO/IEC 20944-1:2013, 3.21.12.21, modified.]

3.15
structured data
data which are organized based on a pre-defined (applicable) set of rules.

Note 1 to entry: The predefined set of rules governing the basis on which the data are structured needs to be clearly stated and made known.

Note 2 to entry: A pre-defined data model is often used to govern the structuring of data.

Note 3 to entry: Examples of structured data are the data contained in relational databases.

[SOURCE: ISO/IEC 20546:2019, 3.1.35, modified.]

4 Foundations

4.1 Context

4.1.1 The data deluge

As organizations create, process and share ever more data, they run the risk of being overwhelmed by a data deluge. Due to rapid growth in global data volumes, any attempted quantification risks becoming quickly obsolete; nevertheless, some indications are available.

The World Economic Forum (WEF) has estimated that the global volume of data will double between 2018 and 2022 and with then double again within 3 years. Currently, much of this growth is driven by searches (5 billion per day) and social media platforms (Twitter: 456 thousand tweets every minute), while future growth is expected to be driven mainly by new data scenarios, especially those related to big data, artificial intelligence (AI) and Internet of Things (IoT).

As data has proliferated, it has become a key enabler for the effective operations of all organizations and critical for effective decision-making by both managers and governing bodies. The pervasiveness of data in organizations today mandates the governance of data as an organizational imperative.

As a consequence, managers and governing body members should seek to better acquaint themselves with the potential value, risk and constraints associated with data.

4.1.2 The strategic value of data

More and more organizations understand that data constitutes a strategic asset which has financial and non-financial value, and which can be used in turn to generate additional value for the organization. Hence the focus on enabling organizations to leverage the value of their data without incurring data/privacy breaches, unethical use, disclosing intellectual property, or having its data misappropriated or misused.

Each organization should consider the data opportunity relative to its strategic context, the nature of the data in its custody, and the risk appetite as defined by the organization's governing body.

4.1.3 The risks associated with data

While data presents an organization with strategic, value-generating opportunities, it can also pose significant threats. Data can be exposed to inappropriate or illegal access and used for illegal purposes. It can be lost and, as a result, expose natural and legal persons to threats against them. It can even be used against the organization itself in anti-competitive, unethical, or illegal ways.

Each organization should consider the threats posed by data in its care, assess the risks and take steps to appropriately address these risks.

4.1.4 Consequences of failure

Ineffective data stewardship by the organization can present very real threats to the organization. Examples include:

a) Data breach litigation: with potentially significant penalties, including legal prosecution and financial penalties. The full cost of a data breach can last for months or even years.

b) Critical failure: disclosure of information, for example via a data breach, that can result in financial loss, the failure of critical infrastructure or, in the most serious cases, to loss of life.

c) Reputational risk: reputation matters in many ways, for example, the ability to recruit top talent or to retain the trust of customers, regulators, investors and other stakeholders.

d) Under-performance: poor data stewardship by the organization can lead to under-performance of the organization and put it at a disadvantage relative to peers or competitors.

4.2 Data classification

There are many ways to organize data. A data taxonomy organizes data into various groups or hierarchies based on a desired facet of data. For example, data can be organized into sub-groups based on the nature of what the underlying data describes (data categories), or based on geo-location of data, or the level of de-identification performed on the data, or on the legal means of control over the data.

Another important facet of data is its level of classification. The classification level describes the significance or sensitivity of the data, from the perspective of an organization. For example, it can be described as *N* levels of significance (*N* being scenario-specific). Data sensitivity, and its associated degree or level, is determined by the purpose and context of the organization and relates to the potential value, risk and constraints of the data. Different classifications allow the organization to have differentiated policies and associated controls and costs based on the data's significance. This ensures each class of data receives the appropriate treatment (e.g. level of security controls or compliance requirements).

See ISO/IEC 19944-1 for a description of a multi-faceted data taxonomy, where data classification is one such facet. ISO/IEC 19944-1 describes how data classification is an important facet in an otherwise broader, multi-faceted taxonomy of data. It is important to note the distinction between data classification and data categorization; the latter refers more to the nature of the data. Some examples that illustrate this distinction are shown in Table 1.

Table 1 — Distinguishing data classification and data categories

Data category: examples	Data classification: examples
Customer data, e.g. identity data, descriptive data	High business impact (HBI), medium business impact (MBI), low business impact (LBI).
Aggregated data, e.g. summary statistics	Confidential, restricted, internal use, public
Derived data, e.g. telemetry	
Anonymized data, so that it is impossible to re-identify an individual	
Structured data, e.g. stored in a structure such as a database	

4.3 Purpose of classification:

Data classification provides a means for the organization to objectively distinguish between different datasets, so as to indicate the significance of the data and to allow differentiated policies and controls consistent with the significance of the data and with its compliance obligations. Data classification is a fundamental requirement for many effective data stewardship activities in an organization.

Some examples of policies and controls that can be applied differently to different classification levels include:

a) Data Protection: This ensures that a risk-based approach is taken for each different classification of data such that treatments are appropriate, cost effective and enable the achievement of the organization's strategic objectives.

b) Compliance: Applying the correct compliance processes for each classification helps to ensure the policies and controls for that level are correctly implemented.

c) Intended use: A core tenet of data stewardship is that data is used only for legitimate and agreed purposes. That means that data can be used or processed only for the purpose explicitly stipulated in an agreement with, and under the parameters defined in, the data agreement. Data classification provides a useful mechanism that ensures that definitive and unambiguous details are assigned to

data attributes such that they are easily understood by people and systems with which they come into contact.

d) Data quality: Data classification (along with data categorization) can help to ensure the necessary treatment of that data to confirm that the appropriate level of data quality is maintained.

e) Innovation: Given the rapidly evolving data landscape, with emerging data scenarios, it is important that the organization considers innovation in its data classification schemes. For example, Internet of Things, artificial intelligence and big data scenarios could test established policies and controls of data assets by the organization.

4.4 Engage and empower staff

Whether through their action or inaction, understanding or misunderstanding, staff of the organization exert a powerful influence over the effective control of the data for which the organization has responsibility. The organization should embark on an open, transparent and consistent dialogue with staff on data issues, to ensure that:

a) they understand the objectives of implementing data classification;

b) they are clear how the supporting processes and systems operate;

c) they understand their roles and responsibilities in the processes, and in delivering the objectives.

The staff engagement process should begin with new hires and continue with a regular communication cycle to all levels of the organization when changes are planned, or when particular issues arise.

4.5 Structure of this document

This document builds on the earlier publications in the ISO/IEC 38500 family of documents focused on IT and Data Governance, and on work on data categorization (see ISO/IEC 19944-1).

— Clause 5 provides an overview of roles and responsibilities between the members of the governing body and managers.

— Clause 6 sets out a framework for completing a data classification.

— Clause 7 specifies supporting principles and considerations.

5 Roles and responsibilities

5.1 General

The roles of both the governing body and management in the governance of IT have been set out in the governance of IT framework in ISO/IEC 38500:2015, Figure 1, reproduced here in Figure 1 for convenience.

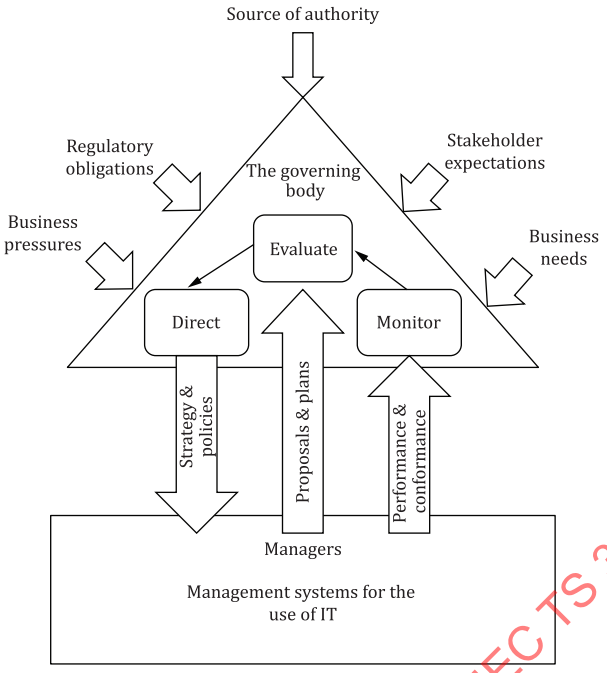

Figure 1 — Governance of IT framework (ISO/IEC 38500)

Figure 2 shows that the governing body is responsible for the data strategy and data policies for the organization and that these align with the overall organizational strategy. It is the management that is responsible, within their delegated authority, for implementation of the policy.

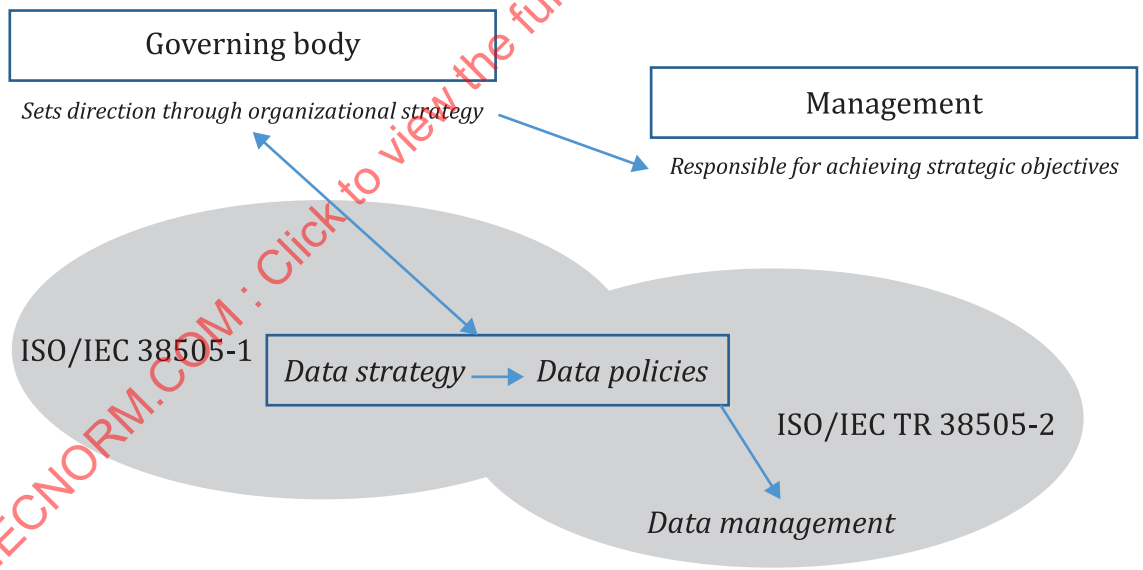

Figure 2 — Role of the governing body and management (ISO/IEC 38505-1 and ISO/IEC TR 38505-2)

5.2 Role of governing body

5.2.1 General

As an enabler of effective data stewardship, and in accordance of ISO/IEC 38500 and ISO/IEC TR 38505-2, the governing body should ensure that the understanding and need for data classification is well established. In this regard, the governing body should:

a) ensure that the role of data in the organization's strategy is understood;

b) maintain good governance of data, consistent with the strategy and risk appetite of the organization;

c) apply data classification principles to effect good data governance.

These items are discussed in more detail in the following subclauses.

5.2.2 Understanding the role of data

The use of data plays an important role in the organization's pursuit of its purpose. The governing body should ensure that it maintains a clear understanding of the importance of data, and of data classification to the organization's strategies as well as the potential strategic value and risk to the organization from the use, or misuse, of that data classification.

5.2.3 Governance of data

The governing body should ensure good governance of data, as it relates to:

a) the value of the data;

b) risks associated with different classes of data;

c) constraints on the use of the data, e.g. regulations, legislation, ethical considerations and contractual obligations.

See ISO/IEC 38505-1.

The governing body should ensure the organization has well-defined policies for data classification within the overall data policy which can include, for example, stakeholder requirements such as compliance with national and international laws, together with regulations and norms, especially those dealing with privacy and security matters.

5.2.4 Data classification approach

The governing body should establish and sustain the enabling environment which ensures that all stakeholders are identified and are aware of their roles and responsibilities (see ISO/IEC TS 38501).

5.2.5 Data classification and risk management

Data presents both threats and opportunities for organizations as have been described previously. The governing body should ensure that the organization is suitably equipped to effectively take opportunities and appropriately mitigate threats. This should be done within the governing body's adopted approach for risk management in the organization.

The governing body should:

a) delegate the responsibility and authority to managers within the organization to ensure risks associated with specific data are aligned to the organization's data classification approach;

b) direct the organization to use the adopted data classification approach to determine risk treatments which are appropriate for the various data classifications; and

c) monitor the organization's risk management results as they are reported in line with the adopted data classification approach.

5.2.6 Direct according to policy

With the organization's data policy and resulting data classification approach in place, the governing body should direct managers to implement the scheme.

Organizational policy should undergo a periodic review process to accommodate changing environments such as changes in regulations and contractual obligations around data sharing, or changes in the use of data or its value to the organization.

5.2.7 Monitor conformance and performance

The governing body should establish oversight mechanisms for the governance of data classification that are appropriate to the level of organizational use of data and compliance with organizational policy.

The governing body should ensure that an appropriate framework is in place for the governance of data classification.

The governing body should monitor the effectiveness of the mechanisms for the governance and management of data classification by requiring processes, such as audit and independent assessments, to gain assurance that the governance is effective and evolves to remain relevant to the emerging needs of the organization.

5.3 Role of management

5.3.1 General

The role of the organization's managers is to fulfil the data classification responsibilities delegated to them by the governing body, and to report to the governing body on their performance and conformance in this regard.

5.3.2 Setting the scope of data classification

Define the goals, objectives, and strategic intent behind the data classification. This helps the organization to stay focused. An organization's objective of the data classification can be to support its compliance obligations, for example, within the European Union's General Data Protection Regulation (EU GDPR).

5.3.3 Propagating and implementing policy

5.3.3.1 Inside the organization

When members of staff encounter data, it should be clear to them what is required to treat the data in a manner consistent with the data classification system:

a) via marking or labelling: what rules apply to the data;

b) via training and communication: the duties and responsibilities of the staff member.

5.3.3.2 Outside the organization: data sharing across supplier and/or partner ecosystem

In situations where data is propagated outside the organization, for example, to a data processor, the same or equivalent protections should be afforded at the destination as at the source. Normally these protections are included in a data sharing agreement between the parties involved.

5.3.4 Defining roles and responsibilities

5.3.4.1 General

Roles and responsibilities should be defined to implement data classification policy. Types of roles and responsibilities include:

— user: an employee authorized to access data for the purpose of processing;

— data custodian: an employee who has administrative or operational responsibility of the organization's data;

— data steward: a senior level employee who makes decisions on how to fully implement the data classification;

— data quality owner: a senior level employee accountable for the quality of one or more datasets;

— internal auditor: an employee who is responsible for the auditing of the multi-faceted taxonomy and reviewing the actual classification of assets and the effective functioning of the classification system.

Roles and responsibilities should be reviewed periodically based on changing regulatory and business requirements.

5.3.4.2 Authority

Management should clearly set out the authority that resides at different levels of the organization, and who, in the chain of command, has ultimate authority to handle un-expected issues that can arise.

5.3.4.3 Enforcement

Management should clearly set out the enforcement measures, such as audit, reporting and escalations. Potential enforcement actions can include issuing an improvement notice or a prohibition notice.

5.3.5 Mobilizing the organization in support of the policy

5.3.5.1 Training

All employees, both new and existing, need to be informed about the data classification to ensure they understand:

a) the underlying policies and compliance issues, for example, involving the GDPR;

b) the objectives of organization's data classification and what safeguards are in place;

c) the organization's expectations for handling data and the employees' specific responsibility in that regard.

5.3.5.2 Communication

Management should keep the organization fully appraised of successes and failures and issues that arise concerning data classification. This can be conducted within an existing regular communications cycle with staff, or with occasional dedicated communications as issues arise, or where key changes are happening within the data classification system.

5.3.6 Operation

5.3.6.1 Defining the performance indicators

The general criteria for performance indicators apply, i.e. that they should flow from the data strategy, they are relevant and simple to monitor and to understand over a period so as to allow trend analysis.

5.3.6.2 Feedback loop

Outputs of the performance indicators, in the form of a report or scorecard, should flow to the individual with ultimate authority for data classification to determine if the system is operating effectively.

5.3.6.3 Performance evaluation

Output reports and scorecards provide the basis for determining the effective operation of the system, at a moment in time, and as a trend to show overall progress over time and to highlight if the processes are operating as required.

5.3.6.4 Plan and implement improvement actions

Where issues or adverse trends are identified, investigations to establish root causes should be undertaken and remedies identified.

5.3.7 Feedback from management to the governing body

5.3.7.1 Reporting

A reporting format and rhythm should be defined and agreed between the governing body and management. The governing body may choose to assign responsibility to one of its sub-committees, for example, its audit and risk committee, in order to provide additional focus.

5.3.7.2 Proposals from management: changes and improvements

Based on experience of operating the data classification scheme, it can be necessary for management to propose changes or improvements. A clear summary of the new issue, together with some potential solutions and a recommendation, should be prepared for consideration by the governing body.

5.3.7.3 Requested guidance for new situations

From time to time, it can be necessary for management to seek additional guidance from the governing body. A clear summary of the new issue, together with some potential solutions and a recommendation, should be prepared for consideration by the governing body.

5.3.8 Levels, discovery and attribution

Management is responsible for the discovery and inventory of all the data assets under its stewardship, and for assigning a data classification attribute or level which describes the significance or sensitivity of the data from the perspective of the organization and using data classification hierarchies defined by the organization.

5.4 Changing classifications

The data landscape is changing rapidly as new data scenarios emerge. Thus, from time to time, it can be necessary to consider updating the existing data classification scheme to reflect:

a) changing needs of customers or data stakeholders;

b) new usage scenarios, for example, in IoT and AI;

c) new regulatory or legal requirements;

d) new issues or risks that emerge, for which the current classification scheme proves to be inadequate;

e) versioning: so as to have traceability of any changes applied to the data classification scheme.

Updating can involve limited change: for example, the overall scheme structure remains unchanged, but particular data sets have to be re-classified. Alternatively, updating can involve more significant change, where the data classification scheme requires re-design which impacts all the data sets over which the organization has custody. This latter change would require, in the first instance, design and consideration of a revised data classification model followed by dialogue across the full range of the organization's data stakeholders about the proposed changes and how and when they will be implemented.

5.5 Defining the requirements: key considerations

Key considerations when defining the requirements include:

a) satisfying legal, regulatory and contractual obligations;

b) fitness for purpose: reflecting the organization's scale, complexity and unique data context, for example, a hospital would have a very different context to a social club;

c) ease of implementation.

6 Data classification framework

To assist organizations in data classification, especially when it is necessary to share data with a third party, a data classification framework is suggested.

Figure 3 shows that the three phases, context, identification and implementation, are sub-divided into activities that are connected by the continuous monitor and improve phase.

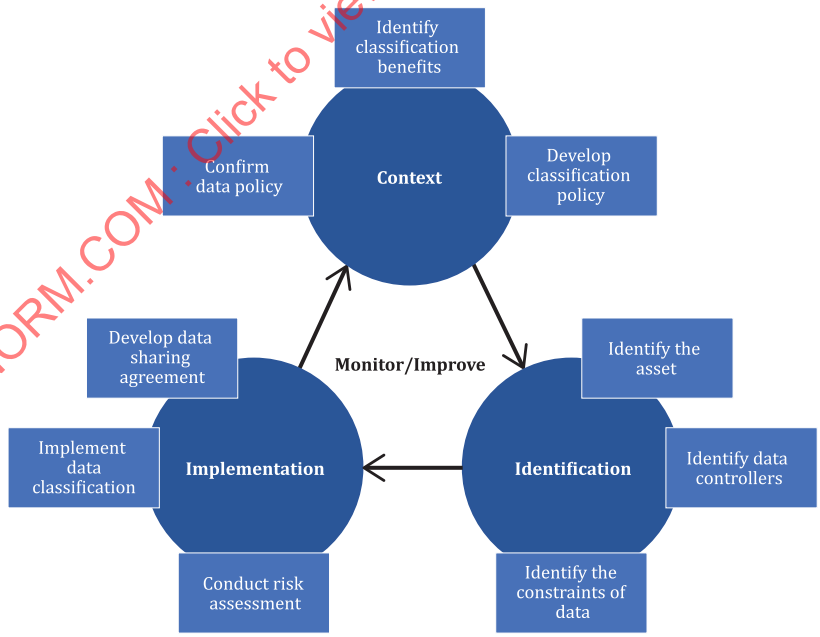

Figure 3 — Data classification framework

6.1 Context

The first phase consists of setting the context necessary to conduct the process of classifying data.

— **Confirm data policy**

The use of data by the organization is critical to achieving its purpose, so the first phase is to understand how the organization intends to use data. In particular, the organization needs to understand the potential value, risks and constraints in its use of data.

— **Identify classification benefits**

Data classification allows the application of different policies and controls on different classes of data. This can improve the efficiency of data treatment and ensure the appropriate resources are allocated in accordance with the significance of the data. Such resources can be directed towards mitigating risk, ensuring better access to the data as well as enabling better return of the investment in data. Identifying the potential benefits and costs of data classification is an important step in setting the context of the data classification framework.

— **Develop a classification policy**

If the organization does not already have a classification policy implemented in this step it can develop one in order to follow the correct procedures and to decide, for example, the roles, responsibilities, permissions and rights for each data classification.

6.2 Identification

The goal of this phase is to identify relevant components to conduct the classification process.

— **Identify the assets**

In order to conduct the classification process, first the organization needs to identify the data that is going to be classified. In this step, organizations need to pay special attention to any data that will be shared with third parties, but also files and documents that are going to be created together.

— **Identify the data controllers**

To continue the process, it is necessary to identify the data controllers, as they are responsible for deciding how the data is going to be used.

— **Identify the constraints on the data**

The use of data can be constrained by policy, laws or stakeholder obligations or expectations. Some examples include constraints on the physical location of the data and its jurisdiction, copyright limitations on its use, privacy requirements and contractual obligations. It is therefore important to identify such constraints on data use as part of the classification process.

6.3 Implementation

This phase is to put into practice the classification process.

— **Conduct risk assessment**

In this step the organization is going to conduct a risk assessment based on the data and risk classifications identified in the previous steps. It also is relevant to consider the data that is going to be shared, to evaluate the risks and the consequences involved.

— **Implement data classification**

In this activity, the data classification policy will come into effect, with handling and disposal procedures being implemented based on the requirements specified in previous activities.

— **Develop data sharing agreement**

This is the phase used for the organization to make a formal data-sharing agreement with third parties based on the data requirements identified in the previous steps.